Introduction

Kernel is a set of DHCP software utility programs that provides an interface between operating systems, DHCP application packages, and users. A key component of Kernel is Sign-on/Security. Kernel's security features are grouped into four chapters in this manual:

- **User Security**
- **Menu Management**
- **Audit Features**
- **Package Integrity**

The purpose of Kernel's security modules is to restrict access to the DHCP computer system to only authorized users, to restrict authorized users to those tasks (menus/options) which they need to perform their jobs, to monitor user actions, to monitor selected changes to the database, and to monitor changes to programs. As such, Kernel offers the system-wide protection of all data on a DHCP system.

All DHCP applications make use of Kernel's security features to segregate functions among employees. For example, the IFCAP (Integrated Funds Distribution, Control Point Activity, Accounting and Procurement) software package uses security keys to distinguish options that only Control Point Officials may use. Many applications now use the Electronic Signature feature as a validation of user identity when sensitive or privileged actions are required (e.g., Order Entry/Results Reporting, Radiology, and IFCAP use the Electronic Signature to approve/verify orders and results). All applications now employ the Program Integrity Checker to determine if the package programs have been altered. Kernel's security features are central to the operation of the DHCP system.

It is important to note first that all DHCP applications offer some package-specific security features. For example, the Pharmacy applications all record the identification of the user who enters a medication order. The IFCAP package records all the users who affect an order for procurement of goods, including Control Point users, the Purchasing Agent, the Accounting Technician, and the Warehouse staff. Many packages preserve the original data as entered by the user and record updates to the data as amendments or adjustments, thereby preserving the data for both legal and retrospective review. Therefore, the ISO should also work with the Application Coordinators at the facility so that the inherent security of the DHCP system as a whole is protected.

The reader is also encouraged to review the other DHCP manuals, especially the *VA FileMan User Manual*, the *Kernel Systems Manual*, and the *MailMan*

***User's Manual*. Review of the Technical Manuals for VA FileMan, Kernel, and MailMan is also suggested.**

This manual addresses Kernel in terms of its security features. The material presented is intended for users whose primary interest is ADP (Automated Data Processing)-based information security. In this manual you will learn how to:

- **Control user security**
- **Manage menus and options**
- **Establish and review audits**
- **Perform program integrity checks**

This manual discusses each of these security tasks, devoting one chapter to each. Each chapter provides you examples of the use of the options within each section. You are encouraged to begin with the section Kernel Security During User Sessions in Chapter 1 to ensure that you first understand the general operation of Kernel.

Package management is not an issue for the Information Security Officer. Responsibility for management of this and other parts of Kernel rests with IRM (Information Resources Management) Service. Information about overall Kernel package management can be found in the *Kernel Systems Manual* and *Kernel Technical Manual*.

Orientation

This manual serves as your Security Features User's Guide. Together with the *Kernel Technical Manual*, it also serves as a Trusted Facility Manual.

The intent of this manual is to provide a guide to the use of the security features supported by Kernel. In essence, this manual can serve your IRM Service and Information Security Officer (ISO) as a Trusted Facility Manual.

This manual focuses on those security features which make up the System Security options of Kernel. Specific procedural instructions are restricted to examples. Users are expected to use the options described in the manual to enhance the ADP Security operations for their facility. In the dialogues that are presented, the user's response is highlighted with bold-faced text.

There is no attempt to cover all possibilities that each option may offer. Rather, examples are shown which illustrate the potential use of Kernel's security features.

Specific details regarding the precise steps Kernel executes to provide system security are not discussed. The actual locations on your DHCP computer system where Kernel records security-related data are not covered. To review such information, please read the *Kernel Systems Manual*.

The reader is encouraged to work closely with the Information Resource Management (IRM) Service to gain an understanding of the parameters and layout of the facility computer system before exercising the options. The more familiar you are with your own computer system, the more information you will gain from the reports produced by these security options.

The reader is also encouraged to become familiar with the security features of other DHCP packages. Many DHCP applications include security features which can assist the Information Security Officer in monitoring system security.

Package Management

Throughout this manual, advice and instruction are offered about the numerous tools Kernel provides for overall DHCP management. Site parameters, for example, are discussed in various sections; information about managing computer security is discussed throughout. The *Kernel Installation Guide* also includes information about package management, such as recommended settings for site parameters and scheduling time frames for tasked options. The *Kernel Systems Manual* also contains extensive information about managing and running Kernel.

To protect the security of DHCP systems, distribution of this software for use on any other computer system by DHCP sites is prohibited. All requests for copies of Kernel for non-DHCP use should be referred to the DHCP site's local ISC.

Otherwise, there are no special legal requirements involved in the use of the Kernel.

Chapter 1: User Security

User security is the cornerstone of Kernel's system security features. This chapter discusses the ways in which the DHCP computer system recognizes and screens users. The following topics are addressed:

- **Kernel Security During User Sessions**
- **Kernel Security Codes**
- **General Advice for Users**
- **Reviewing Users**

Kernel Security During User Sessions

Device Check

A user session begins when a user presses the return or enter key on their terminal. This simple step activates the Security features of Kernel. First, the Kernel determines the device being activated and recognizes it as the user's terminal. The Kernel then reviews the parameters for that device. Among other things, the Kernel notes if the device is permitted to support users at that time. The first step of security is to assure that the device can be used.

User Identification

The Kernel next queries the user for identification. This is done as a two-step procedure. First, the user is prompted to provide an access code. This is followed with a prompt for the user's verify code. The user must provide a valid pair of codes before the DHCP system will allow the user to perform any other actions. Both the access and verify codes that make up the pair must be valid. If the codes entered do not constitute a valid pair, the DHCP system will simply inform the user that the pair is invalid, but will not say which of the two codes, if either, is valid. Thus, the secrecy of both codes is maintained against inappropriate use.

If the user does not enter valid codes, the DHCP system re-prompts the user for the codes. This is repeated until either:

- **The user finally enters a valid pair of codes. Then the Kernel proceeds to offer the user a set of authorized options.**
- **The user continues to attempt to enter valid codes, gives up, or enters an up-arrow ("^") to exit from the sign-on process.**
- **The DHCP system determines that the maximum allowable number of attempts has been exceeded and locks the device. Now the device cannot then be used by anyone until the Kernel determines that the lockout time has passed. The number of attempts is established by IRM Service. This may vary among devices. Typically for a remote device such as a modem, the number of attempts is set to a low value (e.g., three) so that the potential for mischievous or malicious hackers to gain access to your system is minimized. After the Kernel has locked a device, it can record the codes used for the repeated attempts. This is known as the Failed Access Audit. You can establish the detail which your DHCP system records for these events through the option: Establishing Kernel Audit Parameters.**

Menus and Options

Once the user is successfully recognized and signed on to the DHCP system, a set of options is presented on the screen. These options are grouped into menus. Each user has a primary menu, which should reflect the duties that user needs to perform. For example, the primary menu for an Information Security Officer will probably be "System Security Options". This menu leads the user to other menus and options which cause the computer to perform specific operations. Sometimes, the options within a menu are locked with a security key. This key is essentially a second level of security. The user can only use a locked option if they have been given the appropriate key. If the user does not have the key, then even if the locked option is on the user's menu, they will not be able to use it. Options that provide specialized or supervisory access are usually locked with a security key.

Many options update data in the DHCP system. Kernel and VA FileMan control these updates. VA FileMan is the database management system that defines data files and governs data input and reporting. Kernel and VA FileMan provide security controls to restrict data manipulation. Access authority can be defined for each user and can be temporarily granted through the use of options. The following types of access can be granted:

Read	**Allows a user to read data from a file.**
Write	**Allows a user to update the data in a file.**
Delete	**Allows a user to permanently remove data from a file.**
LAYGO	**Allows a user to create a new entry when editing a file. (A special form of write.)**
DD	**Allows data dictionary access for changing or deleting the structure of the file itself (data dictionaries define what types of data are stored, where they are stored, and the relationships among the data fields).**
Audit	**Allows a user to define how a file is audited by VA FileMan.**

Changes are made to data dictionaries by the IRM staff either to install authorized changes or to alter locally developed DHCP applications.

The data on your DHCP system can be very strictly protected. Each user is granted the access needed to perform a job. At the same time, users are prohibited from reviewing or altering data not essential to their tasks.

While users are working with the DHCP system, it monitors some of their activity. The Kernel is able to record the use of all options that the user activates. Thus, the Kernel can track the use of sensitive options. This capability can also be used to determine which options are most frequently used.

The Kernel registers if the user is inactive for a pre-determined length of time. If the user does not interact with the DHCP system within the time-out period, Kernel returns them to the previous prompt, eventually terminating the session of the user. By automatically logging out inactive users the DHCP system limits the possibility that unattended terminals are not used by others.

The Kernel facilitates the activities of all users while simultaneously providing essential security. The sections that follow describe how to use the security features of the Kernel to monitor your DHCP system.

Kernel Security Codes

The first line of security that the Kernel employs is to ensure that only authorized users may access a DHCP computer system. This is done with the security codes of your system. These codes are known as access and verify codes and Electronic Signature. The first two are employed to recognize users. The Electronic Signature is a secret password that some users employ to sign documents via the computer. It is used by many DHCP Applications as an additional security check for sensitive operations.

Access/Verify Codes

With each sign-on, the user must enter two codes to be recognized and allowed to proceed. These codes are the access and verify codes.

The Access Code is assigned by IRM Service. This code is used by the computer to recognize the user. Each user has a unique access code. The only way this code can be changed is for the IRM Service to edit it. When the code is established by IRM, it is encrypted, i.e., it is scrambled according to a cipher. The code is stored in the computer only in this encrypted form. Thus, even if the access code is viewed, the viewer cannot determine what the user actually types to tell the computer this code.

The Verify Code is also generally assigned by the IRM Service. Like the access code, the verify code is also encrypted. This code is used by the computer to verify that the person entering the access code can also enter a second code correctly. Thus, this code is used to determine if the user can verify who they are. After being given access and verify codes, the user can change the verify code at any time. This is done through the Edit User Characteristics menu, which is found in the Toolbox menu (the Toolbox menu can be accessed by entering two question marks (??) at the menu prompt.) It is important to note that the DHCP system requires users to change their verify code on a regular basis. The frequency of changing these codes is set in the KERNEL SYSTEM PARAMETERS file. Security policy states that codes should be changed at least every 90 days.

If IRM Service assigns only the access code, then the first time the new user signs on to your DHCP system, the Kernel prompts them to establish a verify code. The user cannot proceed with the session until this code is entered and validated by the Kernel.

Your system allows access/verify codes to be from 6 to 20 characters in length. The code must contain at least one alpha and one numeric character and may not include the characters "^", ";", ":", or "-". The verify code cannot be the same as the access code. These restrictions are enforced whenever access or verify codes are created or changed. Users should avoid codes that offer no secrecy, such as a child's or spouse's name, a phone number or license plate. If desired, the system can automatically generate codes for your users. These

auto-generated codes resemble automobile license plates (e.g., ABC123). However, they are often difficult for users to remember.

For both the access and verify codes, it is important to remember that there is no way for you to see the codes that were entered for any user. If users forget their access or verify codes, you must assign replacement codes.

Each time users sign on, they see a dialogue similar to the following (depending on the unique physical characteristics of your system):

```
Volume set: VAH     UCI: VAH      Device:  _LTA9130: (VAH604/LC-1-1)

ACCESS CODE:  <enter access code, it will not be displayed on screen>
VERIFY CODE:  <enter verify code, it will not be displayed on screen>
GOOD MORNING  Jim     YOU LAST SIGNED ON TODAY AT 8:30
You have 3 new messages.
```

When the system prompts for the access and verify codes, the text that the user types does not appear on the terminal screen. So, even if someone is watching a user sign on, the codes are not shown. If the user enters codes that the system recognizes as valid, it greets the user and proceeds according to the privileges that are assigned to that user.

If the user fails to enter a set of codes that the system recognizes, the user sees a dialogue as follows:

```
Volume set: VAH     UCI: VAH      Device:  _LTA9130: (VAH604/LC-1-1)

ACCESS CODE:  <enter access code>
VERIFY CODE:   <enter verify code>
Not a valid ACCESS CODE/VERIFY CODE pair


Volume set: VAH     UCI: VAH      Device:  _LTA9130: (VAH604/LC-1-1)

ACCESS CODE:  <enter access code>
VERIFY CODE:   <enter verify code>

GOOD EVENING  Jim     YOU LAST SIGNED ON TODAY AT 17:24

There was 1 unsuccessful attempt since you last signed on:
```

Notice that the computer tells the user that the pair of codes was not valid. It does not specify that the access code was bad or that the problem was with the verify code. Thus, a potential hacker is not given any clues as to whether they are closing in on a valid account.

Take another look at the sign-on dialogue. Notice that the computer tells the user when they last signed on to the system. By asking each user to pay attention to this greeting, you can enlist them in the security process. If the computer reports to a user that they were signed on the day before, and the

user knows that they were not at work, then they can report that information as a possible security violation.

If the user fails to gain access (i.e., multiple unsuccessful attempts are made in succession), then the device may lock. When the device locks, then no user can log onto the system through that device until either the lockout time expires or IRM Service intervenes. The device lockout time is defined in the KERNEL SYSTEM PARAMETERS file as a system default but may be overridden by a lockout time which IRM Service associates with a specific device (e.g., a modem).

Electronic Signatures

A primary aspect of security in many DHCP packages involves the use of Electronic Signatures. Individuals in the system who have authority to approve actions, at whatever level, can enter and edit their own Electronic Signature code. This code is required before data may pass from one level of processing to another. An example of this is the release of a Request for Purchase (Form 2237) in IFCAP. The Control Point Official must first enter their Electronic Signature before the request will be passed to Personnel Property Management for review and processing by Acquisition and Material Management Service.

Like the access and verify codes used when gaining access to the system, the Electronic Signature code will not be visible on the terminal screen. These codes are also encrypted so that even when viewed in the NEW PERSON file by those with the highest levels of access, they are indecipherable.

Electronic Signatures may be established in two ways. The IRM Service can enter a code for the user. Alternately, the code can be left blank and the user can establish it the first time the code is required. The Kernel will inform the user that a code is required and the user must enter one in order to proceed.

Like the verify code, the user may change their Electronic Signature at any time. The Kernel provides an option for the user to do this. Those application packages that allow Electronic Signatures may also include this option for the appropriate class of users.

General Advice for Users

It is important that all users be educated as to how they can assist with ADP Security.

Users should be instructed that when performing basic tasks at a computer terminal, they will probably enter or review information that may be considered sensitive. As a result, protecting security codes is a crucial part of each user's job. Whether it is called an access code, a verify code, or a logon code, security codes are the first line of defense against unauthorized users who may seek to defraud the VA or compromise its computer system. To protect security codes, teach your users to always comply with the following guidelines:

- **Don't share access and verify codes with anyone.**
- **Don't tape access and verify codes under a desk, on a wall, on a terminal, or in other obvious hiding places.**
- **Don't leave the terminal unattended while you are signed on. Sign off each time you leave your terminal unattended.**
- **Don't use obvious codes such as your name and date of birth or your child's name and date of birth.**
- **Don't forget to protect all printouts, computer documents, and media containing sensitive data.**
- **Don't use the computer for personal business.**
- **Do change your security codes at regular intervals. Changing security codes regularly reduces the likelihood that an unauthorized user will detect a unique code.**
- **After signing on, you have a limited amount of time to enter data at any one prompt. If you fail to enter information within an allotted time period, you will be returned to the Select Option prompt. There, Kernel again waits for you to enter information. Should you fail once again to respond within the allotted time period, the computer will ask if you want to HALT. Failure to say No at this level causes the computer to log you off the system.**

Reviewing Users

Your DHCP computer system probably has hundreds, if not thousands, of authorized users. As was discussed in the section Kernel Security During User Sessions, each user has a primary menu. This menu leads the user to the various options that they can invoke on the computer.

It is important to review the access each user has on your computer system. Among the items to check are:

- **Does this user still require access to the computer?**
- **What files/data can this user access?**
- **Is the user's access level appropriate?**
- **If the user has changed departments, has their primary menu been updated to reflect new duties?**

Using the Kernel Security options described in this chapter, you can gather the information to address the above questions. But remember, the Kernel cannot tell you if the access is appropriate, it can only report the current access privileges for the users.

General Information About Users

The List Users option lists all users alphabetically. It shows each user's name, user number, the primary menu option, and the last date/time the user signed on to your system. The user number is used by the computer to uniquely distinguish users.

■ List Users Report

```
Select System Security Option:  REV <RET> iew Users

Select Review Users Option: LIST <RET> users
START WITH NAME: FIRST// A <RET>
GO TO NAME: LAST// AZ <RET>
DEVICE: <RET>
```

```
USER LIST                                        MAR 11,1992  10:48    PAGE 1
                                                              LAST SIGN-ON
NUMBER    NAME                      PRIMARY MENU OPTION     DATE/TIME
------------------------------------------------------------------------------

69        AARDVARK,JOE              PRCSP CLERK             MAR  7, 1992 13:50
12        AHA,EUREKA                XMUSER                  MAR 10, 1992 10:17
42        ANDREW,BUZZ               PSG FILE                MAR 10, 1992 10:30
50        ATEST,ROB                 SDAPP                   MAR  8, 1992 15:03
```

The User Inquiry option displays various attributes for a specific user. If the user is currently signed on, it displays the job and device numbers, the sign-on time, the secondary menu, and the option and menu path currently being used by that individual. Otherwise, it shows the last sign-on time. It also displays the security keys held by the user. This option may be tailored by the IRM staff, so the example below may not exactly match that shown by your system.

■ User Inquiry Report

```
Select Review User Option:  US <RET>er Inquiry
Select NEW PERSON NAME:  TESTER,JOE <RET>

TESTER,JOE  (#23)
------------------------------
Job: 576727625 (22602A49) on ISC,ISC:ISC6V3 from APR 26, 1992@16:41:18
Device: _LTA9130:  (ISC604/LC-1-1)
    Menu path:
           ISC MANAGER'S OPTION
                  Systems Manager Menu
                         System Security
                                Review Users
                                       User Inquiry


ATTRIBUTES
----------------------
Creator    BROWN,BUSTER   Date entered   Aug 1, 1986
Primary menu      EVE     Fileman code(s)      @
    Time-out      300     Type-ahead     Y
Title      Programmer     Office Phone   x1234
Auto-Menu  NO MENUS GENERATED    Last Sign-on   Apr 26, 1992

Secondary Menu Options
-------------------------------------

    TalkMan
    Connect to IDCU Network
    Project Management Menu

Keys Held
---------------
    XMMGR  XUMGR  XUPROG        XMNET  XUPACK
    ZTMQ   XUSER  XMTALK XUPROGMODE
    XMPRIORITY    XUAUDITING    XUARCHIVE
```

You can generate a User Status Report at any time. This report shows the current users who are signed onto the system. For each user, the job number, device, time they signed on and the option they are currently using are displayed. (The job number is an identification the computer employs for the duration of a user session.)

■ User Status Report

```
Select Review Users Option:  User S <RET> tatus Report
Lookup pass .........
MAR 11, 1992  12:51    USER STATUS REPORT      VAH,VAH         PAGE 1

JOB NUMBER  USER NAME        TIME ON  DEVICE  CURRENT MENU OPTION
----------  ---------------  -------  ------  -------------------
22602A49     SAMPLE,FRED     10:50    _LTA9145:User Inquiry
23897A44      TESTER,JOE     10:52    _LTA9130:User Status Report
47582B99     DUCK,DONALD     10:53    _LTA9270:Print Bill
```

You can also locate an active user on the system by using the Find User option. The user must be in the same account (or UCI) as you are. If the user is also on the same CPU, then you will be shown the user's menu path (i.e., all the options that user activated to get to the one they are currently using).

■ Find a User Option

```
Select Review Users Option: FIND <RET> a user
Find User: TESTER,JOE <RET>

User: TESTER,JOE is found on;
Job: 576727625 (22602A49) on ISC,ISC:ISC6V3 from APR 26, 1992@16:41:18
Device: _LTA9130:  (ISC604/LC-1-1)
    Menu path:
       ISC MANAGER'S OPTION
           Systems Manager Menu
                  System Security
                         Review Users
                                Find a user

DONE
```

User's Access to VA FileMan Files

Ordinarily, access to data on the system is controlled through Menu Manager and the assignment of options. Users should only be assigned options that are appropriate to their duties. For example, most pharmacy users would have access to some subset of the pharmacy package options. Then, any data that can be accessed through the pharmacy options, can be accessed by pharmacy users. So access to data in VA FileMan files is ordinarily controlled by the assignment of options.

There is a special set of options, however, that let users manipulate data directly, not through any package; this set of options is part of the VA FileMan package itself. These VA FileMan options let users directly view, modify, and print data from VA FileMan files, as well as modify the file structure itself. For users who have VA FileMan options in their menu tree, it is obviously important to control what access they have to files so that they do not have inappropriate access to view and modify data and files.

Access to VA FileMan files can be controlled in two ways; which way is used at your site depends on whether Kernel's optional File Access Security system has been enabled at your site. If it has not been installed, access is controlled by a user's File Manager access code. If the File Access Security system has been installed, access is controlled by entries in each user's ACCESSIBLE FILE multiple in their NEW PERSON file entry.

Has the File Access Security System been Enabled?

To determine if the File Access Security system has been installed, you can check with your IRM Service. You can also look at the Review Users menu. If the Access to VA FileMan Files option is present, and not marked out of order, that usually indicates that File Access Security system has been installed.

If the File Access Security System Has Not Been Enabled

If Kernel's File Access Security system has not been enabled on your system, a user's access to VA FileMan files through VA FileMan options is controlled by their File Manager access code. You can determine a user's File Manager access code from the User Inquiry report, in the Attributes section; it is the character string listed as "FileMan code(s)".

Each VA FileMan file can have an access code associated with each of six types of access to the file (Read, Write, Delete, LAYGO, DD, and Audit). A user can only access a file in one of these ways if a character in the user's File Manager access code matches the security code associated with that type of access for the file. The exception is if the user has a File Manager access code of "@", programmer access, which enables access of all types to all files.

For more information on file security based on File Manager access code, please see the *VA FileMan User Manual*.

If the File Access Security System Has Been Enabled

If Kernel's File Access Security system has been enabled, a user's access to VA FileMan files through VA FileMan options is controlled by what files are listed in that user's ACCESSIBLE FILES multiple, in their NEW PERSON file entry.

To see which VA FileMan files a user may access when Kernel's File Access Security system has been enabled, use the option Inquiry to a User's File Access. This option displays the files a user can access, showing the user's level of access (e.g., READ, DELETE) for each file. The report also shows users who have programmer access to all files (which means that the user's File Manager access code is set to "@"). In our examples below, we can see that Fred Sample has specific access to two files. On the other hand, the user Bill Trustworthy has programmer mode access and so has access to all files.

■ Example of a User with Access to Two Files

```
Select Access to VA FileMan Files Option:INQ <RET> uiry to a User's File
Access

Select USER NAME: SAMPLE, <RET> FRED

DEVICE:  PRINTER-1 <RET>
```

```
USER ACCESS TO FILES     MAR 16,1992   18:15  PAGE: 1
SAMPLE,FRED  (11) DD     DELETE LAYGO  READ   WRITE  AUDIT
-------------------------------------------------------------------------
3.1       TITLE                YES    YES    YES    YES
3.2       TERMINAL TYPE  YES    YES    YES    YES    YES
```

Example of a User with Programmer Access to All Files

```
Select Access to VA FileMan Files Option: INQ <RET> uiry to a User's File
Access

Select USER NAME: TRUSTWORTHY,BILL <RET>

DEVICE:  PRINTER-1 <RET>
```

```
USER ACCESS TO FILES     MAR 16,1992   18:16  PAGE: 1
TRUSTWORTHY,BILL  (00)   DD     DELETE LAYGO  READ   WRITE  AUDIT
-------------------------------------------------------------------------------

Programmer Access to All Files
```

Sometimes, it is most useful to determine first if the focus should be on a specific set of files, then look at file access to those files. The List Access to Files by File number option lists, by file number, those users who have access to those files. For each type of access (e.g., READ, DELETE), the user's authority is listed. Thus, if a user has YES listed under the WRITE column of this report then that user can, via VA FileMan, write data into the file.

Listing Access by File

```
Select Access to VA FileMan Files Option: L <RET> ist Access to Files by
File number
START WITH WHAT FILE: INSTITUTION// 3.2 <RET>  TERMINAL TYPE    (112 entries)
GO TO WHAT FILE: TERMINAL TYPE// 3.5 <RET> DEVICE    (195 entries)
DEVICE: PRINTER-1 <RET>
```

```
USER ACCESS TO FILES     MAR 11,1992   10:57  PAGE: 1
    USER #     NAME      DD     DELETE LAYGO  READ   WRITE  AUDIT
-------------------------------------------------------------------------------
    FILE:  3.2
           2  BEAR,YOGI               YES    YES    YES    YES
           7  TESTER,JOE  YES    YES    YES    YES    YES
           9  SAMPLE,FRED         YES    YES    YES    YES    YES

    FILE: 3.4
           7  TESTER,JOE  YES    YES    YES    YES    YES
           9  RELIABLE,BETTY      YES    YES    YES    YES    YES

    FILE: 3.5
           7  TESTER,JOE  YES    YES    YES    YES    YES    YES
```

The Print Users Files option lists, by user, each file the user has access to and what that access is (e.g., READ, DELETE). Users who have no access are not listed.

■ Listing File Access for Multiple Users

```
Select Access to VA FileMan Files Option:  Pr <RET> int Users Files
START WITH NAME: FIRST// TESTER <RET>
GO TO NAME: TESTERZ <RET>
DEVICE: PRINTER-1 <RET>
```

```
USER ACCESS TO FILES     MAR 11,1992   10:59  PAGE: 1
    FILE #     ACCESSIBLE FILE   DD     DELETE LAYGO  READ   WRITE  AUDIT
-------------------------------------------------------------------------------

TESTER,JOE     (7)
3.2            TERMINAL TYPE                 YES    YES    YES
3.4            COMMUNICATIONS    YES    YES  YES    YES    YES
3.5            DEVICE                  YES   YES    YES    YES
```

For more information about Kernel's File Access Security system, please see the File Access Security chapter of the *Kernel Systems Manual*.

Chapter 2: Menu Manager Security

This chapter discusses the methods of managing user security by use of the Menu Manager. The following topics are addressed:

- **Examining Menus and Options**
- **Secure Menu Delegation**

Menu Manager provides user-oriented menus that present the user with a selection of the activities they are authorized to perform on your DHCP computer system.

In most cases, users have a set of options that are organized into a menu. Each menu may contain other menus or options that the user employs to perform tasks. Some menus or options have a security key. For these options, the user must hold the key or the option cannot be executed by that user. Moreover, the auto-menu and single-question-mark menu displays don't list locked options, so users ordinarily don't know that the locked option is available, even if it is grouped within a menu for that user. A double-question-mark menu display is needed to show the presence of the locked option. Thus menus on your system are used to grant privileges to users.

Many of the security options available on your system either audit option use or display user options as part of their reports. Therefore, it is important that you become familiar with the tools and options you can use on your system and how they are assigned.

Examining Menus and Options

The Option Access By User option shows you which users can actually access and activate an option. You will be prompted for the name of an option. You will also be asked if you want to see menu paths. Menu paths are all the options that the user must select to actually get to the option you have selected to review. In the example below, only one menu path is shown. Those users must first pick the option EVE (Systems Manager Menu), then XUTIO (Device Handler) to get to XUDEV (Device Edit).

```
Select System Security Option:  MENU <RET> Management Review

Select Menu Management Review Option:  Option <RET> Access By User

Select OPTION NAME: DEVICE EDIT <RET>  XUDEV        Device Edit

Show menu paths? NO// Y <RET>  (YES)
DEVICE: HOME// PRINTER-1 <RET>
```

```
ACCESS TO 'Device Edit'  [XUDEV]

USER NAME              LAST ON          PRIMARY MENU          PATH(S)
---------              -------          ------------          -------
SAMPLE,FRED                   03/10/92         EVE                          1
TESTER,JOE                    03/11/92         EVE                          1

------------------------------    MENU PATH(S)     --------------------

1.  EVE ... XUTIO ... XUDEV
```

Obviously it is difficult to make sense of an option just by seeing its name (XUDEV, for example) and sometimes the associated text does not help significantly (Device Edit). The option to display information about a given option is called Inquire. By using Inquire, you can review an option. The display shows everything recorded about the characteristics of that option. If the option requires a security key, you will see a label LOCK and immediately to the right of that label will be the key which locks that option. There will also be many fields which may seem cryptic and confusing (e.g., DIC {DIC}). These fields are used by the Kernel to affect the actions which the option requires. A more comprehensive discussion of these fields can be found in the *VA FileMan Programmer Manual*.

```
Select Menu Management Review Option:  Inquire <RET>

Which OPTIONS item to display: DEVICE EDIT <RET>  XUDEV        Device Edit
```

```
OPTION LIST                                     OCT  5,1994  14:29    PAGE 1
------------------------------------------------------------------------------


NAME: XUDEV                              MENU TEXT: Device Edit
  TYPE: edit                             CREATOR: POSTMASTER
  HELP FRAME: XUDOC DEVICE LOOKUP        RESTRICT DEVICES?: NO
 DESCRIPTION:   This option will change the device characteristics for a given
 device.
  DIC {DIC}: 3.5                         DIC(0): AEQMLZ
  DIE: 3.5                               DR {DIE}: .01:9999
  TIMESTAMP OF PRIMARY MENU: 54262,51324
  UPPERCASE MENU TEXT: DEVICE EDIT
```

You can also use Print Options File to produce a formatted listing of the OPTION file, showing each option and its associated parameters. You can limit the set of options printed by setting the bounds of your SORT. If you simply press return at the "START WITH NAME: FIRST//" prompt, and accept LAST at the "GO TO NAME: LAST" prompt, you will get all options. On most DHCP systems there are thousands of options. So be warned that choosing all options generates a very large printout.

```
Select Menu Management Review Option:  Print <RET> Options File
SORT BY:  NAME// <RET>
START WITH NAME: FIRST//  XUDEV <RET>
GO TO NAME: LAST//  XUDZ <RET>
       WITHIN NAME, SORT BY:  <RET>
DEVICE:  PRINTER-1 <RET>
```

```
Menu list by display terms  [MENULIST]          MAR 12, 1992   11:27  PAGE 1
MENU TEXT  NAME   TYPE
    DESCRIPTION
------------------------------------------------------------------------------

Device Edit       XUDEV  edit
  This option will change the device characteristics for a given device.

   Edit file:  3.5
  ---------------------------------------------------------------------

Display Device Data      XUDISPLAY     print
  This option is used to print a list of all the devices in the DEVICE
  file.
   Print file: %ZIS (1,
  ---------------------------------------------------------------------
```

As was mentioned at the beginning of this section, the options on your system are organized into menus. One way to view these menus is as an outline that is used to guide the user through their actions. To see these menus in their outline form, use the Diagram Menus option. This option will display in outline form, all of those menus and options that are available to a given user, according to their security and primary menu. These diagrams are generally large, therefore, it is best to request the output to be printed.

Another way of seeing the structure of a menu can be achieved with the Abbreviated Menu Diagrams option. This form provides an abbreviated display of all the options available to a given user, including all menus and options, according to the user's security and primary menu (Option Names, Menu Text, and Synonyms).

Secure Menu Delegation

Your computer system probably has thousands of options. Managing these options and making sure that each user has the options they need to do their job is a time consuming task. To assist your IRM Service in performing this task, Secure Menu Delegation was developed. Secure Menu Delegation allows IRM Service to delegate the task of maintaining the options for each user to a trusted set of other users. From a security perspective, it is important to know who on your system has the privilege of managing menus and options. Secure Menu Delegation provides several options that support this goal.

If you need to review the options that a user may manage, use Show a Delegate's Options. This lists all the options delegated to a specified user. This user can assign which options are to be shown to other users. For each option, the date it was delegated and the user who delegated the option are shown.

```
Select Secure Menu Delegation Option:  SHOW <RET> a Delegate's Options
Select NEW PERSON NAME:  SAMPLE,FRED    <RET>
```

```
SAMPLE,FRED a delegate of: TESTER,JOE on 8/28/91 at level 1

OPTION (INTERNAL #)             MENU TEXT                    DELEGATED    (DUZ)

XUDEV  (93)                     Device Edit                  8/25/91       (22)
XUTERM  (105)                   Terminal Type Edit           8/27/91       (22)
```

You can also use List Delegated Options and their Users. This option produces a list of the options, in alphabetical order, which have been delegated. For each option, the users who have been delegated these options are listed.

```
Select Secure Menu Delegation Option: LIST <RET> Delegated Options and their
Users

DEVICE: PRINTER-1 <RET>
```

```
DELEGATED OPTIONS BY USER                          MAR 11,1992  11:12  PAGE 1
DELEGATED OPTIONS        MENU TEXT                          NAME
------------------------------------------------------------------------------

DG10                     Register Patient                   EXAMPLE,SUE
DG10NOSTAT               10/10 Print, no registrat           EXAMPLE,SUE
XUDEV                    Device Edit                        TESTER,JOE
XUTERM                   Terminal Type Edit                 TESTER,JOE
```

In addition, you can use Print All Delegates and their Options. This report displays, by user, all delegates and their delegated options. For each option, the date it was delegated and the user who delegated it are shown.

```
Select Secure Menu Delegation Option: PRint <RET> All Delegates and their
Options

DEVICE: PRINTER-1 <RET>
```

```
DELEGATED OPTIONS BY USER                    OCT  5,1994  14:32    PAGE 1
                                           CREATION   DELEGATION
NAME                  CREATED BY           DATE            LEVEL
                                               DATE
    DELEGATED OPTIONS     DELEGATED BY         DELEGATED
-------------------------------------------------------------------------------

EXAMPLE,SUE               SAMPLE,FRED          MAY 20,1991       1
    DG10                  0                    MAY 20,1991
TESTER,JOE
    LRZ INQUIRE           SAMPLE,FRED          JUL 21,1994

    LRZ MAIN
```

Chapter 3: Kernel Audit Features

Audit features of the Kernel make it possible to monitor a wide range of computing activity. The following audits are discussed in this chapter:

- **System Access Audits**
- **Option and Server Usage Audits**
- **VA FileMan Audits**

This chapter describes how to use options to set and display audit parameters, initiate audits, print reports, and purge audit logs for these audits.

The security officer and site manager each have interests and responsibilities with system audits. Both are concerned with the prevention of unauthorized access, the exercise of inappropriate levels of access authority, and the potential corruption of the DHCP database through inappropriate alteration of data or dictionaries. Designing and carrying out intelligently planned audits can answer security needs of the facility and help ensure system integrity.

IRM's Responsibility

While maintaining a secure computing environment is the primary responsibility of the Information Security Officer, it is also one of many responsibilities of IRM Service. IRM Service must also attend to problems of system performance such as response time. An audit can degrade response in two ways. The first involves the system resources used to capture audit data during the interactive user session. If a commonly used option is being flagged every time it is invoked, considerable resources will be devoted to the auditing task. The second effect is indirect; as disk space is consumed with audit or other data, an overall slowdown may result as access to a crowded disk with fragmented files takes added time. IRM Service, then, while encouraging the ISO to undertake audits, would also urge that the minimal amount of audited data be collected and that it be purged when no longer needed as an audit trail.

Initiating Audits

One approach to take when embarking on a system review is to examine the existing audit logs that are automatically maintained by the system. These are the Sign-on Log and the PROGRAMMER MODE LOG. Observing daily activity over the course of several weeks will provide a baseline for judging whether an occurrence is unusual. If an unexpected event or trend is seen, an audit can then be undertaken for a specified time period as an investigation. The results may be reviewed, printed if desired, and then purged. The goals of system security as well as system performance may thus be achieved.

When considering an event to audit, research should be done to determine whether a mechanism is already in place within a DHCP application package. The Pharmacy package, for example, may include an option for recording the names of users who approve and verify patient prescriptions. The security measures of other packages should be similarly catalogued. IRM staff and application coordinators will be able to provide this information.

System Access Audits

There are three topics associated with the auditing of system access:

- **Maintaining a list of old access and verify codes.**
- **Recording information about successful sign-on attempts.**
- **Recording information about unsuccessful sign-on attempts.**

Old Access and Verify Codes

As described earlier in this manual, access and verify codes periodically need to be changed. A user may choose a new verify code at any time or may be required to do so if the Lifetime of Verify Code limit has been reached. When a new code is chosen, the old code is kept on file and cannot be reused until the file of old codes is purged.

Preventing reuse of codes is a security measure. A user could otherwise simply change the new code back to the previously used one thus defeating the purpose of requiring the changing of codes. It is wise to retain the list of old codes for some amount of time, but it is also reasonable to purge on occasion. Disk space is one concern. Another is the ease with which users can select new codes, the ones on the list of old codes being unavailable.

Purge

An option for purging the list of old codes is on the System Manager's Manage User File menu. Purging is a function that can be carried out either by IRM Service or the Information Security Officer. An example of the on-line dialogue is as follows:

```
Select User Management Option: Manage User File <RET>

Select Manage User File Option: PURGE <RET> Log of Old Access and Verify Codes

This option will purge the log of old access and verify codes.
It will remove the record of all inactive access and verify codes older
than the date specified and allow for their reuse.

Do you wish to continue? NO// Y <RET>  (YES)

How far back do you wish to retain codes? (7-90 days) 7 <RET>

54 old access codes have been purged.

445 old verify codes have been purged.
```

Sign-on Log

Each time a user successfully signs on, an entry is automatically made in the Sign-on Log.

Print Reports

The Print Sign-on Log option displays the name of the user, the time of sign-on, the device used, and the elapsed time for the session. Note that the elapsed time cannot always be determined. An error may cause an abnormal exit, or the user may be working in programmer mode. Note also that devices will be represented differently according to the system. The following is an example of an on-line dialogue that prints today's (T) log:

```
Select System Audit Reports Option: PRINT <RET> Sign-on Log
START WITH DATE/TIME: FIRST// T <RET>
GO TO DATE/TIME: LAST//   <RET>
DEVICE:   PRINTER-1 <RET>
```

```
USERS WHO HAVE SIGNED ONTO THE COMPUTER       NOV 23,1991 10:15 PAGE 1

                       ELAPSED
SIGNED ON                 TIME
LOCATION             (MINUTES)          USER                   DEVICE
-------------------------------------------------------------------------------
NOV 23,1991  06:20         13           RAMSEY,FRANK           _LTA1903:-ROU
    IRM OFFICE
NOV 23,1991  07:27                      RAWLS,JOHN             _LTA1921:-ROU
    SYSTEMS OFC
NOV 23,1991  08:33         19           ROUSSEAU,JEAN          _LTA1712:-ROU
    MAS OFC #6
NOV 23,1991  09:46         20           RUSSELL,BERTRAND       _LTA1872:-ROU
    MAS OFC #6
NOV 23,1991  10:07                      RYLE,GILBERT           _LTA1900:-ROU
    SYSTEMS OFC
```

Purge

Purging of the Sign-on Log is handled by IRM Service. An option called Purge Sign-on Log is scheduled by IRM Service to run on a regular basis. For example, the purge may run each night and delete all entries over 30 days old, retaining an on-line log of the past 30 days.

Failed Access Attempts

The Failed Access Attempt Log may be used to record information about sign-ons that were attempted but failed. To record information, an audit must be initiated by setting the relevant Kernel site parameters, as shown in the example in the next section, Set Parameters. (If an audit has not been initiated, the Audit Display options described on subsequent pages will show nothing.)

A sign-on attempt fails if the number of permitted attempts is reached and a valid access/verify code pair has not been entered. The number of permitted attempts is a Kernel site parameter, usually set between five and ten. When the limit is reached, an entry is made in the log (if auditing has been initiated). Information is recorded depending upon whether a valid access or verify code was entered during an attempt. If a valid access code is entered, a user name will be associated with the attempt. If requested when establishing the audit parameters, the "text" of any invalid access or verify code attempt will be recorded.

The limit of attempts is usually determined by the Default # of Attempts site parameter. If, however, a limit has been set for a particular device, that limit will take precedence for that device. Such preliminary device checking, though, can be bypassed altogether by using another site parameter, Bypass Device Lockout, which will circumvent the locking mechanism.

When an access attempt fails, the settings for lockout times are checked. If a lockout time is operative for the device, the user must wait for the lockout time to elapse before initiating another sign-on attempt.

Set Parameters

The parameters for the failed access attempt audit are displayed when entering a question mark as shown below. In this case, all devices will be audited and the text entered for invalid access or verify codes will be recorded. Alternatively, audits may be set for specific devices, such as modems or IDCU (Integrated Data Communications Utility) ports that support remote access. (The Option Audit will be discussed subsequently; it is essentially set to NO AUDIT in the example that follows.)

```
Select System Security Option:  AUDIT <RET> Features

Select Audit Features Option: MAINTAIN <RET> System Audit Options

Select Maintain System Audit Options Option:ESTABLISH <RET> System Audit
Parameters
Select KERNEL SYSTEM PARAMETERS DOMAIN NAME: 1 <RET>   VAMC.VA.GOV
INITIATE AUDIT:  T  <RET> (NOV 23, 1991)
TERMINATE AUDIT:  T+7 <RET> (NOV 30, 1991)
OPTION AUDIT: //   <RET>
FAILED ACCESS ATTEMPT AUDIT: ? <RET>
        CHOOSE FROM:
           A      ALL DEVICES/NO TEXT RECORDED
           D      SPECIFIED DEVICES/NO TEXT RECORDED
           AR     ALL DEVICES/TEXT RECORDED
           DR     SPECIFIED DEVICES/TEXT RECORDED
           N      NO AUDIT
FAILED ACCESS ATTEMPT AUDIT: AR <RET>  ALL DEVICES/TEXT RECORDED
```

Initiate/Terminate Audits

The audit will take place if both an initiate and terminate date are specified. Auditing will not occur without specification of a date range. When auditing begins, it proceeds as specified by these parameters, including the Option Audit if it has been specified.

Display Parameters

Parameters for the failed access attempt audit may be displayed as shown below. (Option Audits, if any had been specified, would also be displayed.)

```
Select System Security Option:  AUDIT <RET> Features

Select Audit Features Option: MAINtain System Audit Options <RET>

Select Maintain System Audit Options Option: DISPLAY <RET> the Kernel Audit
  Parameters
SORT BY: NUMBER//  <RET>
    WITHIN NUMBER, SORT BY:  <RET>
DEVICE:  <RET>

List of current Kernel audit parameters
     Initiate on: NOV 23,1991          Terminate on:  NOV 30,1991

     Failed access attempt audit: ALL DEVICES/TEXT RECORDED
```

Print Reports

The Failed Access Attempt Log option displays attempts by date and user, each on a separate page. If a valid access code is entered, the associated user name will be printed. The page may then be taken to the user for verification of identity. If the named individual did not originate the sign-on attempt, it can be assumed that the valid access code has been discovered and a new code should be issued.

Note that if the number of attempts shown exceeds the system limit (default or device-specific), the attempt may not have been initiated by an interactive user. Such an event should be further investigated.

```
Select System Audit Reports Option: FAiled Access Attempts Log <RET>
START WITH DATE/TIME OF ATTEMPT: FIRST// <RET>
    START WITH USER: FIRST//   <RET>
DEVICE: PRINTER-1 <RET>
```

```
LOG OF USER FAILED ACCESS LIST  NOV 23,1991         10:07 AM   PAGE  1
------------------------------------------------------------------------------
           *** USER NAME:   RAWLS,JOHN

DATE/TIME OF ATTEMPT:  AUG 29,1991  15:07
    NUMBER OF ATTEMPTS:     4          TYPE OF FAILED ATTEMPT:  VERIFY
    CPU:  AAA      UCI:  TST           DEVICE: DEC SERVER (DSV2/LC-3-5)
    TEXT ENTERED:
    Verify: IDEALS
    Verify: JUSTICE
```

Failed attempt information may also be displayed for a particular device, as shown below. Devices with a high number of failed attempts should be monitored. Of particular concern would be remote access devices such as modems or IDCU ports.

```
Select Audit Display Option: Device Failed Access Attempts <RET>
DEVICE: PRINTER-1 <RET>
```

```
DEVICE FAILED ACCESS ATTEMPTS       OCT  5,1994           PAGE  1

DEVICE                          DATE/TIME              NUMBER OF ATTEMPTS


DEC SERVER                      AUG 31,1994  15:48            5
DEC SERVER                      SEP  6,1994  10:56            5
DEC SERVER                      SEP  6,1994  11:00            5
DEC SERVER                      SEP  6,1994  11:07            5
DEC SERVER                      SEP 12,1994  15:54            5
DEC SERVER                      SEP 16,1994  13:38            5
DEC SERVER                      SEP 19,1994  07:29            5
DEC SERVER                      SEP 19,1994  08:07            5
DEC SERVER                      SEP 19,1994  15:09            5
DEC SERVER                      SEP 19,1994  15:49            5
DEC SERVER                      SEP 19,1994  15:51            5
DEC SERVER                      SEP 20,1994  10:23            5
DEC SERVER                      SEP 21,1994  14:40            5
DEC SERVER                      SEP 28,1994  11:47            5
DEC SERVER                      SEP 29,1994  09:03            5
DEC SERVER                      OCT  1,1994  18:00            5
                                                            ----
SUBTOTAL                                                      80
                                                            ----
TOTAL                                                         80
```

Failed access attempts may also be displayed by the user name that is associated with the valid access code entered during the failed sign-on attempt.

```
    Select Audit Display Option:  User <RET> Failed Access Attempts
    START WITH USER: FIRST// <RET>
     START WITH DATE/TIME OF ATTEMPT: FIRST// <RET>
    DEVICE:  PRINTER-1 <RET>
```

```
FAILED ACCESS ATTEMPTS                      NOV 23,1991  09:51    PAGE 1
USER                                  DATE/TIME            NUMBER
-------------------------------------------------------------------------
RAMSEY,FRANK    AUG 29,1991  15:25                             5
                                                            ----
SUBTOTAL                                                      5

RUSSELL,BERTRAND   AUG 31,1991  09:58                         4
                                                            ----
SUBTOTAL                                                      4

RYLE,GILBERT                          AUG 29,1991  15:07     2
                                                            ----
SUBTOTAL                                                      2
                                                            ----
TOTAL                                                        11
```

Purge

Purging of the Failed Access Attempt Log is done with an option on the System Security menu as illustrated below.

```
Select Maintain System Audit Options Option: FAILED <RET> Access Attempt Log
Purge

PURGE BEGIN DATE: T-180 <RET>  (SEP 12, 1991)
PURGE END DATE: T-7 <RET>  (MAR 04, 1992)
Requested Start Time: NOW// <RET>  (MAR 11, 1992@10:42)
Request queued
```

Option And Server Usage Audits

There are two files that hold information about the use of options. The first is the PROGRAMMER MODE LOG. The second is the AUDIT LOG FOR OPTIONS. Each is used to store data about when users accessed options.

Programmer Mode Log

All instances of the use of the Programmer Mode option are automatically logged by the system. The file is stored in the Manager's account so that UCI switching can be properly monitored. All instances are audited since this option permits direct system access via the M programming language. Such access is necessary to manage and maintain DHCP packages, but the use of this option should not go without surveillance. Obviously, entry to programmer mode is reserved for your facility's most trusted users only.

Print Reports

The Display of Programmer Mode Entry List option may be used to show the use of programmer mode by user and by date/time. The list may be limited to individual users. The following example shows a list of all users for today (T):

```
Select System Security Option:  AUDIT <RET> Features

Select Audit Features Option:  AUDIT <RET> Display

Select Audit Display Option:  DISPLAY <RET> of Programmer Mode Entry List
START WITH USER: FIRST//  <RET>
      START WITH DATE/TIME: FIRST// T <RET>
      GO TO DATE/TIME: LAST//  <RET>
DEVICE:  PRINTER-1 <RET>
```

```
Programmer Mode Entry List              MAR 11,1992    PAGE  1

DUZ         USER NAME            UCI,VOL        DATE/TIME
-------------------------------------------------------------------------------

13          RAMSEY,FRANK         VAH,ROU        MAR 11,1992  09:38
13          RAMSEY,FRANK         VAH,ROU        MAR 11,1992  15:02
13          RAMSEY,FRANK         VAH,ROU        MAR 11.1992  15:15
13          RAMSEY,FRANK         VAH,ROU        MAR 11,1992  16:46
            --------
SUBCOUNT    4

44          PITKIN,HANNAH        VAH,ROU        MAR 11,1992  10:22
44          PITKIN,HANNAH        VAH,ROU        MAR 11,1992  12:35
            --------
SUBCOUNT    2
            --------
COUNT       6
```

Purge

Although the log of entry into programmer mode is automatically kept, it is not automatically purged. Purging must be done by using the Programmer Mode Entry Log Purge option as shown below:

```
Select Maintain System Audit Options Option: Programmer <RET> Mode Entry Log
Purge

PURGE BEGIN DATE: T-10 <RET>  (NOV 13, 1991)
PURGE END DATE: T <RET>  (NOV 23, 1991)
Requested Start Time: NOW//  <RET>  (NOV 23, 1991@10:42)
Request queued
```

Option Audit

Programmer mode is just one of the many DHCP options. Its importance in terms of access authority justifies automatic auditing of its use. Other options, however, do not need such constant audit.

Set Parameters

When establishing audit parameters, the range of auditing may extend from all options to just a few options. Auditing all options may be of little benefit, not to mention the massive amounts of data that would accumulate. Auditing all options within a namespace should similarly be used only when warranted, for example, to further an investigation. If a problem arose with a particular DHCP package, however, an audit by namespace may be appropriate. For example, auditing the SD namespace would audit the use of all Scheduling options, PRC would audit IFCAP options, and DI would audit VA FileMan options. Or, if concern is with the activity of several DHCP users, the audit may be set to record the option access of those users. Finally, a specific set of options may be identified for auditing.

The example below sets parameters to audit use of VA FileMan's Modify File Attributes option (DIMODIFY) and the Kernel's Device Edit option (XUDEV). It further indicates that all option use by George Boole will be audited, and that all options in the XQSMD namespace, the Kernel's Secure Menu Delegation system, will be audited. (The failed access attempt audit, set in a previous example, will continue to be in effect for the same time period.)

Note that there is a limit to the number of namespaces and users that you can audit at any one time. This limit is due to the fact that all namespaces and users are stored in one limited-length string during audits.

Initiate/Terminate Audits

Auditing will take place during the specified time period. (Auditing will include the failed access attempt audit set in a previous example.) When initiating an audit, review all parameters that have been specified. Any that were specified in the past will again be audited unless they are deleted. For example, if a previous audit had specified other options, users, or namespaces, those would need to be deleted if the current audit was not intended to include them. The Establish System Audit Parameters option may be used to delete prior settings by using the at-sign (@) when prompted with the item to delete.

Set Parameters for Audit

```
Select System Security Option:  AUDIT <RET> Features

Select Audit Features Option: MAINTAIN <RET> System Audit Options

Select Maintain System Audit Options Option: ESTABLISH <RET> System Audit
Parameters
Select KERNEL SYSTEM PARAMETERS DOMAIN NAME: 1 <RET>   VAMC.VA.GOV
INITIATE AUDIT:  T  <RET> (NOV 23, 1991)
TERMINATE AUDIT:  T+7  <RET> (NOV 30, 1991)
OPTION AUDIT: // ? <RET>
     CHOOSE FROM:
       n        NO AUDIT
       a        ALL OPTIONS AUDITED
       s        SPECIFIC OPTIONS AUDITED
       u        USERS AUDITED
OPTION AUDIT: // SPECIFIC OPTIONS AUDITED <RET>
Select OPTION TO AUDIT: DIMODIFY <RET>
    ARE YOU ADDING 'DIMODIFY' AS A NEW OPTION TO AUDIT
     (THE 1ST FOR THIS KERNEL SYSTEM PARAMETERS)?  Y  <RET>  (YES)
Select OPTION TO AUDIT: DEVICE EDIT <RET>  XUDEV           Device Edit
    ARE YOU ADDING 'XUDEV' AS A NEW OPTION TO AUDIT
     (THE 2ND FOR THIS KERNEL SYSTEM PARAMETERS)?  Y  <RET>  (YES)
Select OPTION TO AUDIT:  <RET>
Select NAMESPACE TO AUDIT:  ^OPT <RET>
     1   OPTION AUDIT
     2   OPTION TO AUDIT
CHOOSE 1-2: 1 <RET>
OPTION AUDIT: SPECIFIC OPTIONS AUDITED// USERS AUDITED <RET>
Select USER TO AUDIT: BOOLE,GEORGE <RET>
    ARE YOU ADDING 'BOOLE,GEORGE' AS A NEW USER TO AUDIT
     (THE 1ST FOR THIS KERNEL SYSTEM PARAMETERS)?  Y <RET>   (YES)
Select USER TO AUDIT: <RET>
Select NAMESPACE TO AUDIT: XQSMD <RET>
    ARE YOU ADDING 'XQSMD' AS A NEW NAMESPACE TO AUDIT
     (THE 1ST FOR THIS KERNEL SYSTEM PARAMETERS)?  Y <RET>   (YES)
Select NAMESPACE TO AUDIT:   <RET>
FAILED ACCESS ATTEMPT AUDIT: AR//  ? <RET>
FAILED ACCESS ATTEMPT AUDIT: AR <RET>   ALL DEVICES/TEXT RECORDED
```

Display Parameters

Parameters for the Option Audit are displayed below. Parameters for auditing options as well as parameters for auditing failed attempts will be shown.

```
Select System Security Option:  AUDIT <RET> Features

Select Audit Features Option: MAINTAIN <RET> System Audit Options

Select Maintain System Audit Options Option: DISPLAY <RET> the Kernel Audit
Parameters
SORT BY: NUMBER// <RET>
    WITHIN NUMBER, SORT BY: <RET>
DEVICE: PRINTER-1 <RET>
```

```
List of current Kernel audit parameters
 Initiate on: NOV 23,1991              Terminate on:  NOV 30, 1991
    Option(s) to Audit:  DIMODIFY
    Option(s) to Audit:  XUDEV
    Namespace(s) to Audit: XQSMD
    User to Audit:   BOOLE,GEORGE

Failed access attempt audit: ALL DEVICES/TEXT RECORDED
```

Print Reports

The Audited Options Log option will display information about the audited options. The option name is shown along with the time of use, user, CPU, device, and job number.

```
Select System Audit Reports Option: AUDITED <RET> Options Log
START WITH DATE/TIME: FIRST// <RET>
  START WITH OPTION: FIRST// <RET>
DEVICE:  PRINTER-1 <RET>
```

```
MENU OPTION AUDIT LOG     NOV 23,1991         10:12 AM              PAGE 1
--------------------------------------------------------------------------------
 *** OPTION:  XUDEV
    USER:  LANGER,SUSANNE
DATE/TIME (ENTRY):  OCT 28, 1991  19:21     (EXIT):  OCT 28, 1991  19:23
CPU:  BBB        DEVICE:  89      JOB:          7

 *** OPTION:  XUDEV
    USER:  ROUSSEAU, JEAN-JACQUES
DATE/TIME (ENTRY):  DEC  1, 1991  14:29     (EXIT):  DEC  1, 1991  14:35
CPU:  AAA         DEVICE:  89     JOB:         10
```

Audited options may be displayed sorting by option name and then by date/time. A specific set of options for a particular time period may be shown,

as in the first example below. The audited option log may also be sorted according to users and then by options. The use of options by a particular user may be displayed, as in the second example below.

```
Select Audit Display Option: OPTION <RET> Audit Display
START WITH OPTION: FIRST//   <RET>
  START WITH DATE/TIME: FIRST// <RET>
    DEVICE: PRINTER-1 <RET>
```

```
MENU OPTION AUDIT LIST    NOV 23,1991                                    PAGE  1

OPTION:  XUDEV                                        USER:  RAWLS,JOHN
ENTRY:  OCT 28, 1991  19:21            EXIT:  OCT 28, 1991  19:23

OPTION:  XUDEV                                        USER:  RAMSEY,FRANK
ENTRY:  NOV  1, 1991  14:29            EXIT:   NOV  1, 1991  14:35
```

```
Select Audit Display Option:  USER <RET> Audit Display
START WITH USER: FIRST// BOOLE <RET>
          GO TO USER:LAST// BOOLE <RET>
   START WITH OPTION: FIRST// <RET>
DEVICE:PRINTER-1 <RET>
```

```
USER MENU OPTION AUDIT LIST                          NOV 23,1991    PAGE 1
------------------------------------------------------------------------------
USER:  BOOLE,GEORGE                        OPTION:  XUDEV
ENTRY:  OCT 28,1991  19:21             EXIT:  OCT 28,1991  19:23

USER:  BOOLE,GEORGE                        OPTION:  XUDEV
ENTRY:  NOV 1,1991  14:29              EXIT:  NOV 1,1991  14:35
```

Purge

The Audited Options Log is purged as shown below. This log may need regular purging since it can quickly grow in size with data that is of little significance with respect to auditing.

```
Select Maintain System Audit Options Option: AUDITED <RET> Options Purge
PURGE BEGIN DATE: T-30 <RET>  (OCT 23, 1991)
PURGE END DATE: T <RET>  (NOV 11, 1991)
Request queued
```

Server Audit

Servers are automated mail readers designed to process incoming mail messages, and (possibly) execute routines and options in response to incoming mail messages. To guard against inappropriate server activity, server-type options and server requests should be reviewed and monitored.

The design of server-type options may be reviewed by IRM Service using Menu Management options. Some of the OPTION file attributes to note are the routine and entry/exit actions since they will determine how the server will function. Attributes governing when a server may run are the prohibited times restrictions and the Server Action. The Server Action may be set to honor server requests, ignore server requests, or hold the request and simply notify the mail group associated with the server that a request has been received. Once server activity has begun, a bulletin may be sent to alert the mail group associated with the bulletin. Finally, the server audit flag in the OPTION file may be set for particular server-type options so that an audit trail may be maintained in the AUDIT LOG FOR OPTIONS.

To receive bulletins concerning server activity, the Security Officer will need to contact IRM Service to be added to the mail groups associated with the server bulletins. The default server bulletin is XQSERVER. It will be used unless another bulletin is named in the Server Bulletin field of the OPTION file.

The Information Security Officer may carry out overall audits of server activity by using the option audit techniques described in the previous section of this chapter. The example provided in this section illustrates how to include the auditing of servers in the set of Kernel audit parameters.

VA FileMan audits, described later in this manual, can be used to monitor changes to data in the OPTION file for servers and other options. For example, a data audit could be set for the entry and exit actions to detect any changes.

Set Parameters

All server requests are issued via the Postmaster. The Postmaster exists on each system to manage mail. The Postmaster has a user number of .5 and mail baskets that function as queues for network transmissions. The Postmaster is the "user" of all server requests, so auditing the Postmaster will capture information about server activity.

Auditing the XQSRV namespace will similarly monitor server activity. This is a special case of auditing by namespace. It has been designed to facilitate the auditing of server activity. While specifying a namespace ordinarily sets an audit flag for all options that are named in a particular way (beginning with the characters of the namespace), auditing of the XQSRV namespace

will additionally flag any server-type options, regardless of namespace. It is thus unnecessary to itemize individual server-type options within the multiple of specific options to audit.

The following example illustrates how the Postmaster and the XQSRV namespace may be added to the list of audit parameters to monitor servers.

```
Select System Security Option: AUDIT <RET> Features

Select Audit Features Option: MAINTAIN <RET> System Audit Options

Select Maintain System Audit Options Option:ESTABLISH <RET> System Audit
Parameters

Select KERNEL SYSTEM PARAMETERS DOMAIN NAME: 1  <RET>  VAMC.VA.GOV
INITIATE AUDIT:  T <RET>  (NOV 23, 1991)
TERMINATE AUDIT:  1/1/92 <RET>  (JAN 1, 1992)
OPTION AUDIT: SPECIFIC OPTIONS AUDITED// USERS AUDITED <RET>
Select USER TO AUDIT: BOOLE,GEORGE//  .5  <RET>  POSTMASTER
    ARE YOU ADDING 'POSTMASTER' AS A NEW USER TO AUDIT
     (THE 2ND FOR THIS KERNEL SYSTEM PARAMETERS)?  Y <RET>   (YES)
Select USER TO AUDIT: <RET>
Select NAMESPACE TO AUDIT: XQSMD//  XQSRV <RET>
    ARE YOU ADDING 'XQSRV' AS A NEW NAMESPACE TO AUDIT
     (THE 2ND FOR THIS KERNEL SYSTEM PARAMETERS)?  Y <RET>   (YES)
Select NAMESPACE TO AUDIT:   <RET>
FAILED ACCESS ATTEMPT AUDIT: AR//   <RET>
```

Initiate/Terminate Audits

As stated before, all identified users, options, and namespaces will be audited within the designated time frame. The option to display the Kernel audit parameters may always be used to show what has been specified for auditing. To turn off auditing, it is not enough to simply set the Option Audit flag to No Audit. All items within the user, option, and namespace multiples must be explicitly deleted one by one.

Display Parameters

This display of Kernel audit parameters indicates that server activity will be audited since the Postmaster is audited and the XQSRV namespace is audited. All other operative parameters are also shown.

```
Select System Security Option:  AUDIT <RET> Features

Select Audit Features Option: MAINTAIN <RET> System Audit Options

Select Maintain System Audit Options Option: DISPLAY <RET> the Kernel Audit
  Parameters
SORT BY: NUMBER//  <RET>
    WITHIN NUMBER, SORT BY:  <RET>
DEVICE: PRINTER-1 <RET>
```

```
List of current Kernel audit parameters
  Initiate on: NOV 23,1991             Terminate on:  JAN 1, 1992
    Option(s) to Audit:  DIMODIFY
    Option(s) to Audit:  XUDEV
    Namespace(s) to Audit: XQSMD
    Namespace(s) to Audit: XQSRV
    User to Audit:   BOOLE,GEORGE
    User to Audit:   POSTMASTER

    Failed access attempt audit: ALL DEVICES/TEXT RECORDED
```

Print Reports

The Server Audit Display option lists the audit trail for servers. It shows the option name, the user and sender names, the entry and exit times, and the number and subject of the mail message. In addition, the action taken when the server request was received is shown as a comment. The comment indicates whether the server ran normally or if any errors occurred during the process.

```
Select System Security Option:  AUDIT <RET> Features

Select Audit Features Option: SYSTEM <RET> Audit Reports

Select Audit Display Option:  SERVER <RET> Audit Display

DEVICE: PRINTER-1 <RET>
```

```
                  SERVER OPTION REQUESTS   FEB 26, 1992    17:40

    SERVER OPTION:     ZZSRVTST               USER:  POSTMASTER
ENTRY:     JAN 22, 1992   14:03               EXIT:     JAN 22, 1992    14:03
MESSAGE #:        2922                        SENDER:   PROGRAMMER,CHIEF
SUBJECT:  TEST OF SERVERS

COMMENTS:

Routine ^ZZSRVTST ended normally
```

Purge

Within the specified time range, the audit trail for all options including servers will be purged.

```
Select Maintain System Audit Options Option: AUDITED <RET> Options Purge
PURGE BEGIN DATE: 1/1/92 <RET>  (JAN 1, 1992)
PURGE END DATE: T <RET>  (FEB 26, 1992)
Requested Start Time: NOW//  <RET>  (FEB 26, 1992@18:42)
Request queued
```

VA FileMan Audits

VA FileMan has methods of auditing data values as well as the structural changes to the data dictionaries themselves. A data audit records changes made to the data on file, such as a change in a patient's social security number, the example given in the *VA FileMan User Manual*. A data dictionary (DD) audit, on the other hand, monitors alterations in the data attributes (the definitions of the fields of the file).

For more information and instructions on VA FileMan data audits and data dictionary audits, please see the Auditing chapter of the *VA FileMan User Manual*.

Chapter 4: Package Integrity

Several mechanisms exist to ensure the integrity of the programs of the DHCP system. This chapter discusses four tools that can be used to check the integrity of programs:

- **Program Integrity Checker option**
- **Verify Package Integrity option**
- **Checking Programs Received by Network Mail**
- **Checking Secured Programs Received by Network Mail**

The developers who create the programs that make up the DHCP system have given special consideration to the security needed by the individual packages (e.g., Pharmacy, Laboratory) as well as those of the system at large. The programs written for these packages strictly control the data entered and reviewed by users. In many cases, the programs even mark data with a user's system identification (e.g., DUZ) so that we can determine who entered or changed the data.

But what safeguards are there to be sure no one changes the programs themselves? The first safeguard is obvious. No user should be allowed to enter programmer mode on your system who is not a trusted employee, skilled in the M programming language. On a secure system, the only way such users can enter programmer mode is from the Programmer Mode menu option. Also, security keys must be assigned to such a user to use the Programmer Mode option. And, as you read earlier, every time a user does enter programmer mode through the Programmer Mode option, the system updates the log for that event.

To monitor the integrity of DHCP packages themselves, all DHCP packages are complemented with a program integrity checker. A program integrity checker is basically a table of values with a numeric entry for each program that belongs to a package. The numeric value for a program is the sum of the ASCII values of the characters in that routine. This is an example of a checksum. After the integrity table is built for a package, then those sums can be included with the package. You can compare the sums for components on the current system with the package's original checksums at any time.

For packages created before the advent of the Kernel Installation and Distribution System (KIDS), use the Program Integrity Checker option to verify package integrity. For packages distributed with the new KIDS process, use the Verify Package Integrity option to verify package integrity.

You should not panic if the integrity checker for a package reports a discrepancy (the sums don't match). This does show that a program has been

altered. But usually, the most likely source for the change is that IRM has installed a patch, or correction to the package. IRM updates to a package since the original installation are one cause of mismatches in the checksums.

Program Integrity Checker

The Program Integrity Checker option can be used to run a package-specific integrity checker. It can check package integrity for packages distributed before the advent of the new Kernel Installation and Distribution System (KIDS). For information on how to check package integrity for packages distributed with KIDS, see the description of the Verify Package Integrity option that follows.

With the Program Integrity Checker option, you are prompted for a namespace (e.g., XU for the Kernel). The Kernel then appends the letters NTEG (e.g., XUNTEG). If a program is found that matches the constructed name, that integrity checker is run. The output for a package-specific integrity checker lists the routines included in the package and indicates if the checksum on record matches that of the routine in its current state. Variances between the record and the current routine are flagged on the display. The example below shows a subset of the integrity checker for the Kernel during its development (hence the checker had not been updated to account for the changes made to routine XQ6).

```
Select System Security Option:  Program Integrity Checker <RET>

Select PACKAGE PREFIX: XU <RET>

DEVICE: HOME// <RET>

Running ^XUNTEG...

Checksum routine created on MAR 03, 1992@11:40:57

XQ               ok
XQ1              ok
XQ11             ok
XQ12             ok
XQ1V5            ok
XQ6              Calculated 9993246, off by -5328572
XQ9              ok
XQ91             ok
```

The IRM Service ordinarily runs the Program Integrity Checker each time they load new programs onto your DHCP computer system. This is done to ensure that the newly received programs have not been damaged. Since most of the programs arrive at your facility on diskettes, this is a wise precaution.

Verify Program Integrity

You can use the Verify Package Integrity option to compare checksums of package components against the checksums of the components when they were originally transported. It works only for packages that were distributed using KIDS. For packages distributed before the advent of KIDS, use the Program Integrity Checker option to check package integrity.

Any discrepancies are reported. Currently, routines are the only components that are checked, but checksums will be extended to other package components in the future.

The checksums of components for the currently installed package are verified against checksums stored in the BUILD file entry for the package. If the most recent version of the BUILD file entry for a package has been purged, the Verify Package Integrity option will no longer be able to verify checksums for the loaded package. Because of this, the most recent build entry for a package should not be purged in most cases. For more information on KIDS, see the KIDS section of the *Kernel Systems Manual*.

■ Verify Program Integrity, Sample Run

```
Select Utilities Option: Verify Package Integrity <RET>
Select BUILD NAME: KERNEL 8.0 <RET>
DEVICE: HOME// <RET>


PACKAGE: KERNEL 8.0        Feb 05, 1995 10:02 am                      Page 1
-------------------------------------------------------------------------------

   758 Routine checked, 0 failed.


Select Utilities Option:
```

Checking Programs Received via Network Mail/PackMan

IRM receives new programs via MailMan. Usually, these MailMan messages originate from another computer, most commonly one of the computers at an Information Systems Center. These MailMan messages are received and read just like the conversational messages you routinely exchange. But, instead of regular language, they contain M programs. These are commonly referred to as PackMan messages.

IRM Service uses PackMan messages to update DHCP computer system programs. It is a fast and efficient method to install new programs without the risk of typographical errors. PackMan provides options to construct messages, install messages, and compare messages with programs already installed on your DHCP system. We will not discuss the options to construct or install messages in this manual. Instead, we will concentrate on those options to compare PackMan messages with resident programs.

Why would we want to compare a PackMan message with a resident program? Simply, PackMan offers us another tool to determine if a program on our computer has been altered. If we save the PackMan message, we can compare its contents with our resident programs at any time. So, we always have a ready check against the altering of sensitive programs.

Let's work through an example with the user Joe Tester. Joe will begin by reading his mail and noting that he has three messages in his IN basket. One of these messages, "DEMO PACKAGE FOR MANUAL" contains a PackMan message. After Joe selects that message, MailMan begins to display its contents. As you can see, this is not a regular conversational message. Instead, its contents seem somewhat cryptic. The message begins with a program, called A6SDIOO1.

```
Select System Security Option:  MAILMAN <RET> Menu
MailMan 7.0 service for TESTER,JOE at VAMC.VA.GOV
You last used MailMan: 18 Apr 92 17:51

Select MailMan Menu Option: READ <RET> a message
Read MAIL BASKET: IN//  <RET>
LAST Message Number: 3   Messages in BASKET: 3

IN Basket Message: 1// ? <RET>

*=NEW      ###### Subject ######                    ### From ###
   1. A6SDINIT - Security Demo                     TESTER,JOE
   2. INSTALLATION OF DHCP PACKAGE                 TESTER,JOE
   3. DEMO PACKAGE FOR MANUAL                      SAMPLE,FRED A.
Enter '?HELP' or '???' to see all the other exciting things you can do !

IN Basket Message: 1// 3 <RET>
```

```
Subj: PACKAGE FOR SECURITY DEMO ON 4/14/92  11 Apr 92 10:13  337 Lines
From: SAMPLE,FRED A.      in 'IN' basket.
-------------------------------------------------------------------------------
$ROU A6SDI001
A6SDI001 ;
 ;;Version 1
 F I=1:2 S X=$T(Q+I) Q:X=""  S Y=$E($T(Q+I+1),4,999),X=$E(X,4,999) S:$A(Y)=126
I=I+1,Y=$E(Y,2,999)_$E($T(Q+I+1),5,99) S:$A(Y)=61 Y=$E(Y,2,999) X NO E  S @X=Y
Q Q
 ;;^DIC(16014,0,"GL")
 ;;=^DIZ(16014,
 ;;^DIC("B","SECURITY OFFICER LIST",16014)
 ;;=
 ;;^DD(16014,0)
 ;;=FIELD^^5^6
 ;;^DD(16014,0,"ID",2)
 ;;=S %I=Y,Y=$S('$D(^(0)):"",$D(^DIC(4,+$P(^(0),U,3),0))#2:$P(^(0),U,1),1:""),
C=$P(^DD(4,.01,0),U,2) D Y^DIQ:Y]"" W "   ",Y,@("$E("_DIC_"%I,0),0)") S Y=%I
K %I

Press RETURN to continue or '^' to exit: ^<RET>
```

At this point, Joe enters an up-arrow ("^") to tell MailMan to stop displaying the message. MailMan will prompt the user for an action. In this example, Joe enters "X". This activates PackMan (Note: PackMan is reserved for use by very privileged users only. Joe has a File Manager access code of "@", therefore he can use PackMan.) First, the message is summarized, that is, the contents are itemized.

```
Select MESSAGE Action: IGNORE (in IN basket)// X <RET>
Select PackMan function: SUMMARIZE MESSAGE  <RET>
Line 1     Routine  ROU A6SDI001
Line 57    Routine  ROU A6SDI002
Line 109   Routine  ROU A6SDI003
Line 135   Routine  ROU A6SDI004
Line 181   Routine  ROU A6SDINI1
Line 220   Routine  ROU A6SDINI2
Line 235   Routine  ROU A6SDINI3
Line 279   Routine  ROU A6SDINIT
Line 320   Routine  ROU A6SDM
Line 330   Routine  ROU A6SDP
```

Now that Joe is certain about the content of the PackMan message, he will compare the message contents to the programs that reside on his DHCP computer system. Using PackMan, the Compare option is activated. PackMan now compares the message, line by line, with programs of the same name. Any discrepancies are displayed. In our example below, the program A6SDM does not match. The actual detail shown by PackMan may be difficult for a non-programmer to decipher, but you should discuss such reports with your IRM Service. In all likelihood, the change to the program is appropriate and does not constitute a security violation.

```
Select PackMan function: COMPARE MESSAGE <RET>
DEVICE: HOME//  PRINTER-1 <RET>
```

```
Line 1    Comparing Routine  ROU A6SDI001
-------------------------------------------------------------------------
Line 57   Comparing Routine  ROU A6SDI002
-------------------------------------------------------------------------
Line 109  Comparing Routine  ROU A6SDI003
-------------------------------------------------------------------------
Line 135  Comparing Routine  ROU A6SDI004
-------------------------------------------------------------------------
Line 181  Comparing Routine  ROU A6SDINI1
-------------------------------------------------------------------------
Line 220  Comparing Routine  ROU A6SDINI2
-------------------------------------------------------------------------
Line 235  Comparing Routine  ROU A6SDINI3
-------------------------------------------------------------------------
Line 279  Comparing Routine  ROU A6SDINIT
-------------------------------------------------------------------------
Line 320  Comparing Routine  ROU A6SDM
  1{ ;A6SDM ;ISC - SEND MSG BACK TO }    1{ ;A6SDM ;ISC - SEND MSG BACK TO }
   {SOURCE TO SIGNIFY INSTALL DONE ;}     {SOURCE TO SIGNIFY INSTALL DONE ;}
   {4/18/95  17:56}                       {4/7/95 13:25}
      ^                                      ^
  3{ S A6SD(1,0)="Security Demonstra}    3{ S A6SD(1,0)="Security Demo Pack}
                                ^                                       ^
   {te on Package Installed"}             {age Installed"}
-------------------------------------------------------------------------
Line 330  Comparing Routine  ROU A6SDP
-------------------------------------------------------------------------
Select PackMan function:   <RET>

Select MESSAGE Action: IGNORE (in IN basket)// <RET>  Ignored.
```

Checking Secured Programs Received via Network Mail/PackMan

VA FileMan allows a user to create a PackMan message containing the programs that make up a software package. Under this option, instead of creating programs that are saved on the computer disk, the routines are written directly into a MailMan message (i.e., no routines are written to the disk). The programmer provides a Scramble Hint by which the message is encrypted. When the message is received, the recipient can use the Scramble Hint to decode the package. If the message is intact (i.e., it has not been tampered with), the package can then be installed with the PackMan utilities. The message can also be saved to compare against the routines on the disk at future dates much the same way in which an integrity checker or standard PackMan message is used.

The only major difference with secured messages is that you must first provide the correct scramble password before you can do anything with the message. Let's look at an example. This time, Joe will look at a message titled "A6SDINIT - Security Demo". He uses MailMan as before, enters a password, and proceeds as if this were a standard PackMan message.

```
Select Systems Security Menu Option: MAILMAN <RET> Menu
MailMan 7.0 service for SAMPLE,FRED at KERNEL.ISC-SF.VA.GOV
You last used MailMan: 14 Apr 92 17:39

Select MailMan Menu Option: READ <RET> a message
Read MAIL BASKET: IN//   <RET>
LAST Message Number: 5   Messages in BASKET: 3

N Basket Message: 1// ? <RET>
*=NEW      ###### Subject ######                              ### From ###
   1. ADP SECURITY MEETING                                        DOE,JOHN
   2. INSTALLATION OF DHCP PACKAGE            SAMPLE,FRED
   5. A6SDINIT - Security Demo                                    TESTER,JOE
Enter '?HELP' or '???' to see all the other exciting things you can do !

IN Basket Message: 1// 5 <RET>
```

```
This text was scrambled with the scramble hint: 'DEMO '
Enter scramble password:  <TYPE IN THE PASSWORD HERE>

Subj: A6SDINIT - Security Demo  13 Apr 89 11:21  513 Lines
From: TESTER,JOE      in 'IN' basket.
---------------------------------------------------------------------------
$TXT
$ROU ^A6SDM
A6SDM ;SFISC - SEND MSG BACK TO SOURCE TO SIGNIFY INSTALL DONE
;4/7/89  13:25
;V1
 S A6SD(1,0)="Security Demo Package Installed"
 S XMY(DUZ)="",XMY("G.A6SD INSTALL")=""
 S XMSUB="INSTALLATION OF DHCP PACKAGE: SECURITY OFFICER LIST"
 S XMTEXT="A6SD(" N DIFROM D ENX^XMD
 K XMSUB,XMTEXT,XMY
 Q
$END ROU A6SDM
$ROU ^A6SDP
A6SDP ;SFISC/CNP - PRINT LIST OF SECURITY OFFICERS ;4/5/89  18:55
 ;V1
Press RETURN to continue or '^' to exit:
```

At this point, Joe enters an up-arrow ("^") to tell MailMan to stop displaying the message. MailMan prompts the user for an action. As in the earlier example, Joe enters "X". This activates PackMan (Remember: PackMan is reserved for use by very privileged users only. Joe has a File Manager access code="@", therefore he can use PackMan.) He will simply compare the message contents to the programs that reside on his DHCP computer system. Using PackMan, the Compare option is activated. As before, PackMan compares the message, line by line, with programs of the same name. This time, the programs saved in the PackMan message match those installed on our DHCP computer system.

```
Select MESSAGE Action: IGNORE (in IN basket)// X <RET>   (Typing an X will
                                                          activate PackMan)

Select PackMan function: ? <RET>
 ANSWER WITH PackMan function NUMBER, OR NAME
CHOOSE FROM:
   1           ROUTINE LOAD
   2
      GLOBAL LOAD
   3           PACKAGE LOAD
   4           SUMMARIZE MESSAGE
   5           PRINT MESSAGE
   6           INSTALL MESSAGE
   7           COMPARE MESSAGE

Select PackMan function: COMPARE MESSAGE <RET>
DEVICE: HOME//  <RET>  DECSERVER
```

```
Line 2    Comparing Routine  ROU ^A6SDM
-------------------------------------------------------------------------------
Line 12   Comparing Routine  ROU ^A6SDP
-------------------------------------------------------------------------------
Line 20   Comparing Data Dictionary  DDD ^SECURITY OFFICER LIST
Line 78   Comparing Data Dictionary  DDD ^JOB SERIES
Line 120  Comparing FileMan Data  DTA ^JOB SERIES
Line 142  Comparing Bulletins  BUL ^
Line 156  Comparing Input Templates  DIE ^
Line 162  Comparing Print Templates  DIP ^
Line 184  Comparing Security keys  KEY ^
Line 192  Comparing Options  OPT ^
Line 270  Comparing Package File  PKG ^
Line 374  Comparing Routine  ROU ^A6SDINI1
-------------------------------------------------------------------------------
Line 407  Comparing Routine  ROU ^A6SDINI2
-------------------------------------------------------------------------------
Line 419  Comparing Routine  ROU ^A6SDINI3
-------------------------------------------------------------------------------
Line 460  Comparing Routine  ROU ^A6SDINIT
-------------------------------------------------------------------------------
Line 499  Comparing Routine  ROU ^A6SDNTEG
-------------------------------------------------------------------------------
```

Appendix A: DHCP Security Forms

When a user is granted an account on your DHCP system, two forms are prepared by the Kernel to meet system security policies and procedures. User Account Notification and the Computer Account Access Policy. Upon creation of a new user account, the Kernel will automatically print these forms for the user(s).

The Medical Information Security Service in MIRMO (Medical Information Resources Management Office) has reviewed these documents and their suggested wording is shown below. Your facility may customize these documents to meet your local needs. The documents are stored as Help Frames and can be edited via the Help Frame menu in Kernel.

USER ACCOUNT NOTIFICATION

Department of Veterans Affairs

Your VA Facility
123 Any Address
Anytown, State, Zip

A user account has been created in your name to enable you to access on-line clinical and/or administrative data required to perform your duties as an employee of the Department of Veterans Affairs. Please read the enclosed NEW USER INFORMATION before you attempt your first log-on to the system. Questions about access should be referred to the AIS Application Coordinator in your service, your facility Information Security Officer (ISO), or your IRM Service.

Your Computer Access Coordinator is:

Your Facility Information Security Officer:

Your Alternate Information Security Officer:

COMPUTER ACCOUNT ACCESS POLICY

Department of Veterans Affairs

Your VA Facility

As an authorized user of VHA automated information systems (AISs) and having access to data stored in them, I will be given sufficient access to perform my assigned duties. I will use this access ONLY for its intended purpose and understand the following policies that apply to VA data and computer systems:

I agree to safeguard all passwords (e.g., Access/Verify codes, electronic signature codes) assigned to me and am strictly prohibited from disclosing these codes to anyone including family, friends, fellow workers, supervisor(s), and subordinates for ANY reason.

I understand that I may be held accountable for all entries/changes made to any government AIS using my passwords.

I am aware of the regulations and facility AIS security policies designed to ensure the confidentiality of all sensitive information. I am aware that information about patients or employees is confidential and protected from unauthorized disclosure by law. I understand that my obligation to protect VA information does not end with either the termination of my access to this facility's systems or with the termination of my government employment.

I will exercise common sense and good judgment in the use of electronic mail. I understand that electronic mail is not inherently confidential and I have no expectation of privacy in using it. I understand that technical or administrative problems may create situations which requires viewing of my messages. I also understand that facility management officials may authorize access to my electronic mail messages whenever there is a legitimate purpose for such access.

I understand that a violation of this notice constitutes disregard of a local and/or VHA policy and will result in appropriate disciplinary action as defined in VA employee conduct Regulations (VAR 820(b)) as well as suspension/termination of access privileges.

I affirm with my signature that I have read, understand, and agree to fulfill the provisions of this User Access notice.

Signature:_____

Glossary

Access Code	**A password used along with the verify code to provide secure user access. It is used by the Kernel's Sign-on/Security system to identify the user.**
ADPAC	**Automated Data Processing (ADP) Application Coordinator (see Application Coordinator, below).**
Alerts	**Brief on-line notices that are issued to users as they complete a cycle through the menu system. Alerts are designed to provide interactive notification of pending computing activities, such as the need to reorder supplies or review a patient's clinical test results. Along with the alert message is an indication that the View Alerts common option should be chosen to take further action.**
ANSI	**American National Standards Institute.**
ANSI M	**An implementation of the M computer language that conforms to ANSI standards.**
Application Coordinator	**Designated individuals responsible for user-level management and maintenance of an application package such as IFCAP or Lab. Also abbreviated as ADPAC (ADP Application Coordinator).**
Application Package	**In DHCP, software and documentation that support the automation of a service, such as Laboratory or Pharmacy within VA medical centers (see Package).**
Application Programmer	**The person who writes code for application packages. The Kernel provides tools to facilitate package development.**
Application Programming Interface (API)	**Programmer calls provided by the Kernel for use by application programmers. APIs allow programmers to carry out standard computing activities without needing to duplicate Kernel utilities in their own packages. APIs also further DBA goals of system integration by channeling activities, such as adding new users, through a limited number of callable entry points.**
Array	**An arrangement of elements in one or more dimensions. A MUMPS array is a set of nodes referenced by subscripts that share the same variable name.**

ASCII	**American Standard Code for Information Interchange. A series of 128 characters, including upper and lower case alpha characters, numbers, punctuation, special symbols, and control characters.**
Audit Access	**A user's authorization to mark the information stored in a computer file to be audited.**
Auditing	**Monitoring computer usage such as changes to the database and other user activity. Audit data can be logged in a number of VA FileMan and Kernel files.**
Auto-menu	**An indication to Menu Manager that the current user's menu items should be displayed automatically. When auto-menu is not in effect, the user must enter a question mark at the menu's select prompt to see the list of menu items.**
Backup	**The process of creating duplicate data files and program copies or both as a reserve in case the original is lost or damaged.**
Bug	**An error in a program. Bugs may be caused by syntax errors, logic errors, or a combination of both.**
Bulletins	**Electronic mail messages that are automatically delivered by MailMan under certain conditions. For example, a bulletin can be set up to fire when database changes occur, such as adding a record to the file of users. Bulletins are fired by bulletin-type cross references.**
Callable Entry Point	**An authorized programmer call that may be used in any DHCP application package. The DBA maintains the list of DBIC-approved entry points.**
Capacity Management	**The process of assessing a system's capacity and evaluating its efficiency relative to workload in an attempt to optimize system performance. The Kernel provides several utilities.**
Caret	**A symbol expressed as ^ (caret). In many M systems, a caret is used as an exiting tool from an option. Also known as the up-arrow symbol.**
Checksum	**A numeric value that is the result of a mathematical computation involving the characters of a routine or file.**

Cipher	**A system that arbitrarily represents each character as one or more other characters. See also encryption.**
Command	**A combination of characters that instruct the computer to perform a specific operation.**
Common Menu	**Options that are available to all users. Entering two question marks at the menu's select prompt will display any secondary menu options available to the signed-on user along with the common options available to all users.**
Compiled Menu System (^XUTL global)	**Job-specific information that is kept on each CPU so that it is readily available during the user's session. It is stored in the ^XUTL global, which is maintained by the menu system to hold commonly referenced information. The user's place within the menu trees is stored, for example, to enable navigation via menu jumping.**
Computed Field	**This field takes data from other fields and performs a predetermined mathematical function (e.g., adding two columns together). You will not, however, see the results of the mathematical function on the screen. Only when you are printing or displaying information on the screen will you see the results for this type of field.**
Control Key	**The Control Key (Ctrl on the keyboard) performs a specific function in conjunction with another key. On some systems, for example, Ctrl-S causes printing on the terminal screen to stop, while Ctrl-Q restarts printing on the terminal screen.**
CORE	**The fundamental clinical application packages of the DHCP.**
CPU	**Central Processing Unit. Those parts of computer hardware that carry out arithmetic and logic operations, control the sequence of operations performed, and contain the stored program of instructions.**
Cross Reference	**An indexing method whereby files can include pre-sorted lists of entries as part of the stored database. Cross references (x-refs) facilitate look-up and reporting.**
CRT	**An acronym for cathode ray tube, the basis of the television screen and the standard microcomputer display screen. See also Terminal, Monitor, VDT.**

Data Attribute	**A characteristic of a unit of data such as length, value, or method of representation. VA FileMan field definitions specify data attributes.**
Data Dictionary	**Definition of the structure of a VA FileMan file, its attribute fields, and its relationships with other files.**
Data Dictionary Access	**A DHCP user's authorization to write/update/edit the data format for a computer file. Also known as DD Access.**
Database	**A set of data, consisting of at least one file, that is sufficient for a given purpose. The DHCP database is composed of a number of VA FileMan files.**
DBA	**Database Administrator. In DHCP, the person who monitors namespacing conventions and other procedures that enable various DHCP packages to coexist within an integrated database system.**
DBIA	**Database Integration Agreement. The DBA maintains a list of DBIAs or mutual agreements between package developers allowing the use of internal entry points or other package-specific features that are not available to the general programming public.**
DBIC	**Database Integration Committee. Within the purview of the DBA, the committee maintains a list of DBIC-approved callable entry points and publishes the list on FORUM for reference by application programmers and verifiers.**
Debug	**To correct logic errors or syntax errors or both in a computer program. To remove errors from a program.**
Default Response	**A response considered the most probable answer to the prompt. In DHCP, a default response is identified by double slash marks (//) immediately following it. This allows you the option of accepting the default answer or entering your own answer. To accept the default you simply press the enter (or return) key. To change the default answer, type in your response.**

Delete	**A key on your keyboard that allows you to delete characters. In DHCP, the @ sign (uppercase of the 2 key) may also be used to delete an entire response in a field. The computer will ask "Are you sure you want to delete this entry?" to insure you do not delete an entry by mistake.**
Delete Access	**A user's authorization to remove information stored in a computer file.**
Device	**Terminals, printers, modems and other types of peripheral equipment associated with a computer. An operating system file like the ones found in the VAX computer system may also be considered a device for input/output.**
Device Handler	**The Kernel module that provides a mechanism for accessing peripherals and using them in controlled ways (e.g., user access to printers or other output devices).**
DHCP	**The Decentralized Hospital Computer Program of the Veterans Health Administration (VHA), Department of Veterans Affairs (VA). DHCP application packages, developed within VA, are used to support clinical and administrative functions at VA medical centers nationwide.**
DIFROM	**VA FileMan utility that gathers all package components and changes them into routines (namespaceI* routines) so that they can be exported and installed in another VA FileMan environment.**
Direct Mode Utility	**A programmer call that is made when working in direct programmer mode. A direct mode utility is entered at the MUMPS prompt (e.g., >D ^XUP). Calls that are documented as direct mode utilities *cannot* be used in application package code.**
Double Quote (")	**A symbol used in front of a Common option's menu text or synonym to select it from the Common menu. For example, the five character string "TBOX selects the User's Toolbox Common option.**

DR String	**The set of characters used to define the variable DR when calling VA FileMan. Since a series of parameters may be included within quotes as a literal string, the variable's definition is often called the DR string. To define the fields within an edit sequence, for example, the programmer may specify the fields using a DR string rather than an input template.**
DUZ	**A local variable holding the user number that identifies the signed-on user.**
DUZ(0)	**A local variable that holds the File Manager Access Code of the signed-on user.**
Electronic Signature Code	**A secret password that some users may need in order to sign documents via the computer.**
Encryption	**Scrambling data or messages with a cipher or code so that they are unreadable without a secret key. In some cases encryption algorithms are one directional, that is, they only encode and the resulting data cannot be unscrambled (e.g., access/verify codes).**
Entry	**A VA FileMan record. It is uniquely identified by an internal entry number (the .001 field) in a file.**
Error Trap	**A mechanism to capture system errors and record facts about the computing context such as the local symbol table, last global reference, and routine in use. Operating systems provide tools such as the %ER utility. The Kernel provides a generic error trapping mechanism with use of the ^%ZTER global and ^XTER* routines. Errors can be trapped and, when possible, the user is returned to the menu system.**
Field	**A field is similar to blanks on forms. It is preceded by words that tell you what information goes in that particular field. The blank, marked by the cursor on your terminal screen, is where you enter the information. A reserved area in a record used for storage of specific information.**
File	**A set of related records treated as a unit. VA FileMan files maintain a count of the number of entries or records.**

File Access Security system — Formerly known as Part 3 of the Kernel Inits. If the File Access Security conversion has been run, file-level security for VA FileMan files is controlled by Kernel's File Access Security system, not by File Manager Access codes.

File Manager — See VA FileMan.

Forced Queuing — A device attribute indicating that the device can only accept queued tasks. If a job is sent for foreground processing, the device will reject it and prompt the user to queue the task instead.

Form — See ScreenMan Forms.

FORUM — The central E-mail system within DHCP. It is used by developers to communicate at a national level about programming and other issues. FORUM is located at the Washington, DC ISC (162-2).

Free Text — A type of data field whose permissible values are any combination of numbers, letters, and symbols.

Go-home Jump — A menu jump that returns the user to the Primary menu presented at sign-on. It is specified by entering two up-arrows (^^) at the menu's select prompt. It resembles the rubber band jump but without an option specification after the up-arrows.

Help Frames — Entries in the HELP FRAME file that may be distributed with application packages to provide on-line documentation. Frames may be linked with other related frames to form a nested structure.

Help Processor — A Kernel module that provides a system for creating and displaying on-line documentation. It is integrated within the menu system so that help frames associated with options can be displayed with a standard query at the menu's select prompt.

Help Prompt — Computer assistance available to you at your terminal screen. The Help function assists you with menus and describes options so you can make the proper choice. To get "help" in DHCP, enter 1 to 4 question marks in response to a prompt. The level of help you get increases with the number of question marks you enter.

Hook or Link	**Non-specific terms referring to ways in which files may be related (via pointer links) or can be accessed (via hooks).**
Host File Server (HFS)	**A procedure available on layered systems whereby a file on the host system can be identified to receive output. It is implemented by the Device Handler's HFS device type.**
Hunt Group	**An attribute of an entry in the DEVICE file that allows several devices to be used interchangeably; useful for sending network mail or printing reports. If the first hunt group member is busy, another member may stand in as a substitute.**
IDCU	**Integrated Data Communications Utility; the telecommunications network used to interconnect computers among VA facilities.**
Index (%INDEX)	**A Kernel utility used to verify routines and other MUMPS code associated with a package. Checking is done according to current ANSI MUMPS standards and DHCP programming standards (see SAC). This tool can be invoked through an option or from direct mode (>D ^%INDEX).**
Init	**Initialization of an application package. INIT* routines are built by VA FileMan's DIFROM and, when run, recreate a set of files and other package components.**
Internal Entry Number (IEN)	**The number used to identify an entry within a file. Every record has a unique internal entry number.**
IRM	**Information Resource Management. A service at VA medical centers responsible for computer management and system security.**
ISC	**Information Systems Center.**
ISO	**Information Security Officer. Person responsible for information security at each VA Medical Center. Works in conjunction with Regional Security Officers (RISOs).**

Jump	**In DHCP applications, the Jump command allows you to go from a particular field within an option to another field within that same option. You may also Jump from one menu option to another menu option without having to respond to all the prompts in between. To jump, type an up-arrow (^) -- which is your shift key plus the 6 key -- and then type the name of the field or option you wish to jump to. See also Go-home, Phantom, Rubber Band, or Up-arrow jump.**
Jump Start	**A logon procedure whereby the user enters the "access code;verify code;option" to go immediately to the target option, indicated by its menu text or synonym. The jump syntax can be used to reach an option within the menu trees by entering "access;verify;^option".**
Kermit	**A standard file transfer protocol. It is supported by the Kernel and can be set up as an alternate editor.**
Kernel	**The DHCP package that enables DHCP application packages to coexist in a standard operating-system-independent computing environment.**
Laygo Access	**A DHCP user's authorization to create a new entry when editing a computer file. (Learn As You GO, the ability to create new entries).**
Link or Hook	**Non-specific terms referring to ways in which files may be related (via pointer links) or can be accessed (via hooks).**
Logon	**The process of gaining access to a computer system.**
Logoff	**The process of exiting from a computer system.**
M	**A programming language recognized by the American National Standards Institute. Alternately know as MUMPS; the acronym MUMPS stands for Massachusetts General Hospital Utility Multiprogramming System.**
Mail Message	**An entry in the MESSAGE file. The DHCP electronic mail system (MailMan) supports local and remote networking of messages.**
MailMan	**The Kernel module that provides a mechanism for handling electronic communication, whether it's user-oriented mail messages, automatic firing of bulletins, or initiation of server-handled data transmissions.**

Manager Account	**A UCI that can be referenced by non-manager accounts such as production accounts. Like a library, the MGR UCI holds percent routines and globals (e.g., ^%ZOSF) for shared use by other UCIs.**
MAS	**Medical Administration Service.**
Menu	**A list of choices for computing activity. A menu is a type of option designed to identify a series of items (other options) for presentation to the user for selection.**
Menu Cycle	**The process of first visiting a menu option by picking it from a menu's list of choices and then returning to the menu's select prompt. Menu Manager keeps track of information, such as the user's place in the menu trees, according to the completion of a cycle through the menu system.**
Menu Manager	**The Kernel module that controls the presentation of user activities such as menu choices or options. Information about each user's menu choices is stored in the Compiled Menu System, the ^XUTL global, for easy and efficient access.**
Menu System	**The overall Menu Manager logic as it functions within the Kernel framework.**
Menu Template	**An association of options as pathway specifications to reach one or more final destination options. The final options must be executable activities and not merely menus for the template to function. Any user may define user-specific menu templates via the corresponding Common option.**
Menu Text	**The descriptive words that appear when a list of option choices is displayed. Specifically, the Menu Text field of the OPTION file. For example, User's Toolbox is the menu text of the XUSERTOOLS option. The option's synonym is TBOX.**
Menu Trees	**The menu system's hierarchical tree-like structures that can be traversed or navigated, like pathways, to give users easy access to various options.**
MIRMO	**Medical Information Resources Management Office.**
MIS	**Management Information System.**

Modem — A device for connecting a terminal to a telephone line, allowing it to communicate with another modem.

Monitor — The device on which images generated by the computer are displayed. The term usually refers to a video display and its housing. See also CRT, VDT, Terminal.

Multiple — A multiple-valued field; a subfile. In many respects, a multiple is structured like a file.

MUMPS — See M.

Namespacing — The convention of using a unique 2-4 character prefix for package components like options and routines. The DBA assigns unique character strings for package developers to use in naming routines, options, and other package elements so that packages may coexist. Namespacing includes "number spacing" whereby the files of a package stay within a pre-defined range of numbers.

Node — In a tree structure, a point at which subordinate items of data originate. A MUMPS array element is characterized by a name and a unique subscript. Thus, the terms node, array element, and subscripted variable are synonymous. In a global array, each node might have specific fields or "pieces" reserved for data attributes.

Numeric Field — A data field whose permissible values are limited to numeric characters of a restricted number of digits.

Online — A device is online when it is connected and capable of responding to the computer.

Operating System — A basic program that runs on the computer, controls the peripherals, allocates computing time to each user, and communicates with terminals.

Option — An entry in the OPTION file. As an item on a menu, an option provides an opportunity for users to select it thereby invoking the associated computing activity. Options may also be scheduled to run in the background, non-interactively, by TaskMan.

Option Name — The NAME field in the OPTION file. For example, XUMAINT for the option that has the menu text "Menu Management". Options are namespaced according to DHCP conventions monitored by the DBA.

PAC	**Programmer Access Code. An optional user attribute that may function as a second level password into programmer mode.**
Package	**The set of programs, files, documentation, help prompts, and installation procedures required for a given software application. For example, Laboratory, Pharmacy, and MAS are packages.**
Part 3 of the Kernel Init	**See File Access Security system.**
Password	**A user's confidential sequence of keyboard characters, which must be entered at the beginning of each computer session to provide the user's identity.**
Patch	**An update to a package. Patches can include code updates, documentation updates, and information updates. Patches are applied to the programs on your DHCP system by IRM Service.**
Pattern Match	**A preset formula used to test strings of data. Refer to your system's M Language Manuals for information on Pattern Match operations.**
Peripheral Device	**Any hardware device other than the computer itself (central processing unit plus internal memory). Typical examples include card readers, printers, CRT units, and disk drives.**
Phantom Jump	**Menu jumping in the background. Used by the menu system to check menu pathway restrictions.**
Pointer	**Allows entries in one VA FileMan file to be the field values of another file; this is accomplished by use of a pointer field.**
Primary Menus	**The list of options presented at sign-on. Each user must have a primary menu in order to sign-on and reach Menu Manager. Users are given primary menus by IRM. This menu should include most of the computing activities the user will need.**
Production Account	**The UCI where users log on and carry out their work, as opposed to the manager, or library, account.**

Programmer Access	**Privilege to become a programmer on the system and work outside many of the security controls of Kernel. Accessing programmer mode from Kernel's menus requires having the programmer's at-sign security code, which sets the variable DUZ(0)=@.**
Prompt	**A question or message issued interactively and requiring a response.**
Protocol	**An entry in the PROTOCOL file. Used by the Order Entry/Results Reporting (OE/RR) package to support the ordering of medical tests and other activities. The Kernel includes several protocol-type options for enhanced menu displays within the OE/RR package.**
Queuing	**Requesting that a job be processed in the background rather than in the foreground within the current session. The Kernel's Task Manager handles the queuing of tasks.**
Queuing Required	**An option attribute that specifies that the option must be processed by TaskMan (the option can only be queued). The option may be invoked and the job prepared for processing, but the output can only be generated during the specified time periods.**
Read Access	**A user's authorization to read information stored in a computer file.**
Record	**A set of related data treated as a unit. An entry in a VA FileMan file constitutes a record.**
Required Field	**A mandatory field, one that must not be left blank. The prompt for such a field will be repeated until the user enters a valid response.**
Resource	**A method that enables sequential processing of tasks. The processing is accomplished with a RES device type designed by the application programmer and implemented by IRM. The process is controlled via the RESOURCE file.**
Return	**On the computer keyboard, the key located where the carriage return is on an electric typewriter. It is used in DHCP to terminate “reads”. Symbolized by <RET>.**
RISO	**Regional Information Security Officer. Regional representative of VA Medical Center Information Security Officers (ISOs).**

Routine	**A program or sequence of computer instructions that may have some general or frequent use. M routines are groups of program lines that are saved, loaded, and called as a single unit via a specific name.**
Rubber Band Jump	**A menu jump used to go out to an option and then return, in a bouncing motion. The syntax of the jump is two up-arrows followed by an option's menu text or synonym (e.g., ^^Print Option File). If the two up-arrows are not followed by an option specification, the user is returned to the primary menu (see Go-home Jump).**
SAC	**Standards and Conventions (maintained by the SACC, setting guidelines to be followed by DHCP application programmers).**
SACC	**Standards and Conventions Committee of DHCP. This committee is responsible for maintaining the SAC.**
Scheduling Options	**A way of ordering TaskMan to run an option at a designated time with a specified rescheduling frequency, such as once per week.**
ScreenMan Forms	**A screen-oriented display of fields, for editing or simply for reading. VA FileMan's Screen Manager is used to create forms that are stored in the FORM file and exported with a package. Forms are composed of blocks (stored in the BLOCK file) and can be regular, full screen pages or smaller, pop-up pages for multiples.**
Scroll/No Scroll	**The Scroll/No Scroll button (also called Hold Screen) allows the user to "stop" (No Scroll) the terminal screen when large amounts of data are displayed too fast to read and "restart" (Scroll) when the user wishes to continue.**
Secondary Menus	**Options assigned to individual users to tailor their menu choices. If a user needs a few options in addition to those available on the Primary menu, the options can be assigned as secondary options. To facilitate menu jumping, secondary menus should be specific activities, not elaborate and deep menu trees.**
Secure Menu Delegation (SMD)	**A controlled system whereby menus and keys can be allocated by people other than IRM staff, such as application coordinators, who have been so authorized. SMD is a part of Menu Manager.**

Server	**An entry in the OPTION file. An automated mail protocol that is activated by sending a message to the server with the "S.server" syntax. A server's activity is specified in the OPTION file and can be the running of a routine or the placement of data into a file.**
Set of Codes	**Usually a one- or two-character preset code that is a permissible value for a data field. Almost always, the set of codes data fields require capital letters as a response (e.g., M for male and F for female). If anything other than the acceptable code is entered, the computer will reject the response.**
Sign-on/Security	**The Kernel module that regulates access to the menu system. It performs a number of checks to determine whether access can be permitted at a particular time. A log of sign-ons is maintained.**
Site Manager/IRM Chief	**At each DHCP site, the individual who is responsible for managing computer systems, installing and maintaining new modules, and serving as liaison to the ISCs.**
Software	**The set of instructions and data required to operate the computer. One type is called operating system software -- that is, fundamental computer software that supports other software. The second type is called applications software -- in other words, customized programs that tell the computer how to run applications (e.g., Pharmacy, Laboratory).**
Special Queuing	**An option attribute indicating that TaskMan should automatically run the option whenever the system reboots.**
Spooler	**An entry in the DEVICE file. It uses the associated operating system's spool facility, whether it's a global, device, or host file. The Kernel manages spooling so that the underlying OS mechanism is transparent. In any environment, the same method can be used to send output to the spooler. The Kernel will subsequently transfer the text to a global for subsequent despooling (printing).**
Subscript	**In MUMPS, a numeric or string value that is enclosed in parentheses, appended to the name of a local or global variable, and used to identify a specific node within an array.**

Synonym	**A field in the OPTION file. Options may be selected by their menu text or synonym (see Menu Text).**
TaskMan	**The Kernel module that schedules and processes background tasks (also called Task Manager).**
Templates	**In VA FileMan, a way of associating fields in a file or in related files for later reference. Edit sequences are stored in the INPUT TEMPLATE file, print specifications are stored in the PRINT TEMPLATE file, and search or sort specifications are stored in the SORT TEMPLATE file.**
Terminal	**A device consisting of a video adapter, a monitor, and a keyboard. A terminal does little or no computer processing on its own; instead, it is connected to a computer by a communications link. See also Monitor and CRT.**
Timed-read	**The amount of time the Kernel will wait for a user response to an interactive read command before starting to halt the process.**
Trigger	**A type of VA FileMan cross reference. Often used to update values in the database given certain conditions (as specified in the trigger logic). For example, whenever an entry is made in a file, a trigger could automatically enter the current date into another field holding the creation date.**
Type-ahead	**A buffer used to store characters that are entered before the corresponding prompt appears. Type-ahead is a shortcut for experienced users who can anticipate an expected sequence of prompts.**
UCI	**User Class Identification, a computing area. The MGR UCI is typically the manager's account, while VAH or ROU may be production accounts.**
Up-arrow Jump	**In the menu system, entering an up-arrow (^) followed by an option name accomplishes a jump to the target option without needing to take the usual steps through the menu pathway.**

User Interface — The way the package is presented to the user -- issuing of prompts, help messages, menu choices, etc. A standard user interface can be achieved by using VA FileMan for data manipulation, the menu system to provide option choices, and VA FileMan's Reader, the ^DIR utility, to present interactive dialogue.

VA FileMan — DHCP's Database Management System (DBMS). The central component of the Kernel that defines the way standard DHCP files are structured and manipulated.

VAX — Virtual Address Extension; a computer series manufactured by Digital Equipment Corporation. One of the types of computers used by DHCP.

VDT — Video Display Terminal. (See CRT, Terminal, Monitor.)

Verification — A process of DHCP package review carried out by technical staff not directly involved in the development of the package. Any violations of SAC policy should be identified and corrected.

Verify Code — A secret password used along with the access code to provide secure user access. The Kernel's Sign-on/Security system uses the verify code to validate the user's identity.

Write Access — A user's authorization to write/update/edit information stored in a computer file.

Z Editor (^%Z) — A Kernel tool used to edit routines or globals. It can be invoked with an option, or from direct mode after loading a routine with >X ^%Z.

ZOSF Global (^%ZOSF) — The Operating System File -- a manager account global distributed with the Kernel to provide an interface between DHCP application packages and the underlying operating system. This global is built during Kernel installation when running the manager setup routine (ZTMGRSET). The nodes of the global are filled-in with operating system-specific code to enable interaction with the operating system. Nodes in the ^%ZOSF global may be referenced by application programmers so that separate versions of the package need not be written for each operating system.

Index

Access code 7, 10
- **Format 10**
- **Number of attempts 8**
- **User advice 13**

Audit Features 45
- **Initiate/Terminate 32, 38, 43**
- **Initiating 28**
- **Namespaced options 38**
- **Servers 42**

Audit logs
- **Failed Access Attempts Log 31**
- **Old access and verify codes 29**
- **Sign-on Log 30**

Audit options
- **Display Parameters**
  - **Display the Kernel Audit Parameters 32, 40**
- **Print Reports**
  - **Audited Options Log 40**
  - **Display of Programmer Mode Entry List 36**
  - **Failed Access Attempts Log 33**
  - **Print Sign-on Log 30**
  - **User Audit Display 41**
  - **User Failed Access Attempts 34**
- **Purge**
  - **Failed Access Attempts Log Purge 35**
  - **Programmer Mode Entry Log Purge 37**
  - **Purge Log of Old Access and Verify Codes 29**
  - **Purge Sign-on Log 30**
- **Set Parameters**
  - **Establish System Audit Parameters 31, 38**

Device (locked) 8, 12
Electronic signature code 12
Failed Access Audit 8
Find a User 16
Forms for DHCP security clearance 57
Kernel Audit Features 27
List Access to Files by File Number 19
List Users 14
Locked devices 8, 12
Menu Management 25
- **Diagram Menus 23**
- **Inquire option 22**
- **Option Access by User 21**
- **Print options 22**

Menu Manager Security 21
Menus 8, 21
MUMPS 47
Option Access By User 21
Options 21
Package Integrity 47-55
- **Checksums 47**
- **MailMan 50**
- **PackMan**
  - **Compare 51**
- **Patch 48**
- **Program Integrity Checker 47, 48**
- **Programs 47**
- **VA FileMan 53**
- **Verify Program Integrity 49**

PackMan 50
- **Compare option 51**
- **Summarize option 51**
- **VA FileMan 53**

Primary menu 8
Program Integrity Checker 48
Programmer mode 36
Reviewing users 14
Secure menu delegation 24
- **List Delegated Options & Users 24**
- **Print Delegates & Options 25**
- **Show Delegate's Options 24**

Security codes 10
Security forms 57
Security key 8, 21
Server Audit Display 44
Trusted Facility Manual 3
User Inquiry 15
User Security 7-20
- **Finding on-line 16**
- **Inquiry 15**
- **Inquiry to a User's File Access 18**
- **List Access to Files by File Number 19**
- **Listing 14**
- **Status report 16**

User Status Report 16
VA FileMan
- **Audits 45**
- **File security 8, 17-20**
- **Secured Messages 53**

Verify code 7, 10
- **Format 10**
- **User advice 13**

Verify Program Integrity 49

Department of Veterans Affairs
Decentralized Hospital Computer Program

KERNEL
SECURITY TOOLS MANUAL

Version 8.0

July 1995

Information Systems Center
San Francisco, California

Preface

The purpose of this manual is to provide instructions for Information Security Officers (ISOs) to review the DHCP (Decentralized Hospital Computer Program) system. Material is presented with the assumption that the reader has access to a VA DHCP computing environment with Security Officer access to the Kernel. It is assumed that the reader may not be familiar with the Kernel as a whole but has a basic working knowledge of VA FileMan.

Table of Contents

Introduction 1

Orientation 3

Package Management 5

Chapter 1: User Security 7
- **Kernel Security During User Sessions** 7
  - **Device Check** 7
  - **User Identification** 7
  - **Menus and Options** 8
- **Kernel Security Codes** 10
  - **Access/Verify Codes** 10
  - **Electronic Signatures** 12
- **General Advice for Users** 13
  - **General Information About Users** 14
  - **User's Access to VA FileMan Files** 17

Chapter 2: Menu Manager Security 21
- **Examining Menus and Options** 21
- **Secure Menu Delegation** 24

Chapter 3: Kernel Audit Features 27
- **IRM's Responsibility** 27
- **Initiating Audits** 28
- **System Access Audits** 29
  - **Old Access and Verify Codes** 29
  - **Sign-on Log** 30
  - **Failed Access Attempts** 31
- **Option And Server Usage Audits** 36
  - **Programmer Mode Log** 36
  - **Option Audit** 38
  - **Server Audit** 42
- **VA FileMan Audits** 45

Chapter 4: Package Integrity 47
- **Program Integrity Checker** 48
- **Verify Program Integrity** 49
- **Checking Programs Received via Network Mail/PackMan** 50
- **Checking Secured Programs Received via Network Mail/PackMan** 53

Appendix A: DHCP Security Forms 57

Glossary 59

Index 77